日 本 国 特 許
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application: ２００２年１２月 ６日

出 願 番 号
Application Number: 特願２００２－３５５１１７

[ST.10/C]: [ＪＰ２００２－３５５１１７]

出 願 人
Applicant(s): パイオニア株式会社

２００３年 ６月３０日

特 許 庁 長 官
Commissioner,
Japan Patent Office 太田信一郎

出証番号 出証特２００３－３０５１４５０

【書類名】　特許願

【整理番号】　57P0451

【提出日】　平成14年12月 6日

【あて先】　特許庁長官殿

【国際特許分類】　G09C 1/00

G11B 27/031

【発明者】

【住所又は居所】　埼玉県所沢市花園４丁目２６１０番地　パイオニア株式会社　所沢工場内

【氏名】　吉村　隆一郎

【発明者】

【住所又は居所】　埼玉県所沢市花園４丁目２６１０番地　パイオニア株式会社　所沢工場内

【氏名】　横塚　栄彦

【発明者】

【住所又は居所】　埼玉県所沢市花園４丁目２６１０番地　パイオニア株式会社　所沢工場内

【氏名】　仁田　聡

【特許出願人】

【識別番号】　000005016

【氏名又は名称】　パイオニア株式会社

【代理人】

【識別番号】　100104765

【弁理士】

【氏名又は名称】　江上　達夫

【電話番号】　03-5524-2323

【選任した代理人】

【識別番号】　100107331

【弁理士】

【氏名又は名称】　中村　聡延

【電話番号】　03-5524-2323

【手数料の表示】

【予納台帳番号】　131946

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0104687

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置、情報記録装置、情報記録媒体、コンピュータプログラム及び情報処理方法

【特許請求の範囲】

【請求項１】　情報を再生又は実行するための情報処理装置であって、

前記情報を取得する取得手段と、

前記取得手段により取得された情報の再生処理又は実行処理を行う処理手段と

前記取得手段により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているか否かを判定する暗号化判定手段と、

前記暗号化判定手段による判定の結果、前記取得手段により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときには、前記取得手段による情報の少なくとも一部のさらなる取得を阻止するように前記取得手段を制御し、又は前記取得手段により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように前記処理手段を制御する第１制御手段と

を備えたことを特徴とする情報処理装置。

【請求項２】　前記取得手段により取得された情報の中に所定のフォーマットを有する情報が含まれているか否かを判定するフォーマット判定手段と、

前記フォーマット判定手段による判定の結果、前記取得手段により取得された情報の中に前記所定のフォーマットを有する情報が含まれていないときには、前記取得手段による情報の少なくとも一部のさらなる取得を阻止するように前記取得手段を制御し、又は前記取得手段により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように前記処理手段を制御する第２制御手段と

を備えたことを特徴とする請求項１に記載の情報処理装置。

【請求項３】　前記取得手段により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているときに、その所定の暗号化方式により暗号化された情報を復号化する復号化手段と、

前記復号化手段により復号化された情報が認証情報であるか否かを判定する認証情報判定手段と、

前記認証情報判定手段による判定の結果、前記復号化された情報が認証情報でないときには、前記取得手段による情報の少なくとも一部のさらなる取得を阻止するように前記取得手段を制御し、又は前記取得手段により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように前記処理手段を制御する第３制御手段と

を備えたことを特徴とする請求項１又は２に記載の情報処理装置。

【請求項４】　前記認証情報判定手段は、前記復号化された情報のチェックサムが所定の値か否かを調べることにより、前記復号化された情報が認証情報であるか否かを判定することを特徴とする請求項３に記載の情報処理装置。

【請求項５】　前記復号化手段により復号化された情報が前記認証情報であるときに、前記認証情報が情報記録媒体上の所定のアドレスに記録されているか否かを判定するアドレス判定手段と、

前記アドレス判定手段による判定の結果、前記認証情報が前記所定のアドレスに記録されていないときには、前記取得手段による情報の少なくとも一部のさらなる取得を阻止するように前記取得手段を制御し、又は前記取得手段により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように前記処理手段を制御する第４制御手段と

を備えたことを特徴とする請求項３又は４に記載の情報処理装置。

【請求項６】　前記情報記録媒体には、コンテンツ情報と前記認証情報が記録されており、前記認証情報の前記情報記録媒体上のアドレスには、前記コンテンツ情報の前記情報記録媒体上のアドレスを用いて所定の演算を行うことによって得られる値が設定されており、

前記アドレス判定手段は、前記コンテンツ情報の前記情報記録媒体上のアドレスを用いて前記所定の演算を実行する演算手段と、

前記認証情報の前記情報記録媒体上のアドレスの値が、前記演算手段の演算により得られた値と一致するか否かを比較する比較手段と

を備えたことを特徴とする請求項５に記載の情報処理装置。

【請求項７】　前記復号化手段により復号化された情報が前記認証情報であるときに、前記認証情報が多層情報記録媒体の所定の層に記録されているか否かを判定する記録層判定手段と、

前記記録層判定手段による判定の結果、前記認証情報が所定の層に記録されていないときには、前記取得手段による情報の少なくとも一部のさらなる取得を阻止するように前記取得手段を制御し、又は前記取得手段により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように前記処理手段を制御する第５制御手段と

を備えたことを特徴とする請求項３又は４に記載の情報処理装置。

【請求項８】　前記認証情報は画像情報であることを特徴とする請求項３ないし７のいずれかに記載の情報処理装置。

【請求項９】　前記認証情報はロゴであることを特徴とする請求項３ないし７のいずれかに記載の情報処理装置。

【請求項１０】　前記認証情報のフォーマットはＤＶＤビデオフォーマットであることを特徴とする請求項３ないし７のいずれかに記載の情報処理装置。

【請求項１１】　前記所定の暗号化方式は、鍵を用いて情報記録媒体に記録すべき情報を暗号化し、前記鍵を、前記情報記録媒体の所定記録領域に記録する方式であり、前記所定記録領域は、前記情報記録媒体に記録された情報を読み取る機能を有する一般ユーザ向けの情報読取装置を通常の操作方法で操作することによって任意にアクセスすることができない領域であることを特徴とする請求項１ないし１０のいずれかに記載の情報処理装置。

【請求項１２】　前記所定の暗号化方式はＣＳＳ（コンテント・スクランブル・システム）であることを特徴とする請求項１ないし１０のいずれかに記載の情報処理装置。

【請求項１３】　前記取得手段は、ＤＶＤ－ＲＯＭドライブであることを特徴とする請求項１ないし１２のいずれかに記載の情報処理装置。

【請求項１４】　前記処理手段は、ＭＰＥＧ（Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ）デコードモジュールを備えていることを特徴とする請求項１ないし１３のいずれかに記載の情報処理装置。

【請求項１５】　前記取得手段により取得された情報は、当該情報処理装置で実行可能なコンピュータプログラムを含むことを特徴とする請求項１ないし１４のいずれかに記載の情報処理装置。

【請求項１６】　前記取得手段により取得された情報は、当該情報処理装置で実行可能なゲームプログラムを含むことを特徴とする請求項１ないし１４のいずれかに記載の情報処理装置。

【請求項１７】　請求項１６に記載の情報処理装置を備えたゲーム装置。

【請求項１８】　情報記録媒体上にコンテンツ情報と前記コンテンツ情報が真正なものであることを示すための認証情報とを記録する情報記録装置であって、

前記コンテンツ情報を記録すべき前記情報記録媒体上のアドレスを取得するアドレス取得手段と、

前記アドレス取得手段により取得された前記コンテンツ情報のアドレスを用いて所定の演算を行い、当該演算により得られた値を前記認証情報の前記情報記録媒体上のアドレスの値に設定するアドレス設定手段と、

前記認証情報を所定の暗号化方式により暗号化する暗号化手段と、

前記アドレス取得手段により取得されたアドレスに前記コンテンツ情報を記録し、前記アドレス設定手段により設定されたアドレスに前記暗号化手段により暗号化された認証情報を記録する記録手段と

を備えたことを特徴とする情報記録装置。

【請求項１９】　多層情報記録媒体上にコンテンツ情報と前記コンテンツ情報が真正なものであることを示すための認証情報とを記録する情報記録装置であって、

前記コンテンツ情報を前記多層情報記録媒体のいずれかの層に記録する第１記録手段と

前記認証情報を所定の暗号化方式により暗号化する暗号化手段と、

前記暗号化手段により暗号化された認証情報を前記多層情報記録媒体の層のうち、前記コンテンツ情報を記録する層以外のいずれかの層に記録する第２記録手段と、

を備えたことを特徴とする情報記録装置。

【請求項２０】　コンテンツ情報と前記コンテンツ情報が真正なものであることを示すための認証情報とが記録されたコンピュータ読取可能な情報記録媒体であって、

前記認証情報は所定の暗号化方式により暗号化された状態で記録されており、

前記認証情報の記録アドレスには、前記コンテンツ情報の記録アドレスを用いて所定の演算を行うことによって得られた値が設定されていることを特徴とする情報記録媒体。

【請求項２１】　コンテンツ情報と前記コンテンツ情報が真正なものであることを示すための認証情報とが記録されたコンピュータ読取可能な多層情報記録媒体であって、

前記コンテンツ情報は前記多層情報記録媒体のいずれかの層に記録されており、

前記認証情報は、所定の暗号化方式で暗号化された状態で、前記多層情報記録媒体の層のうち前記コンテンツ情報を記録する層以外のいずれかの層に記録されていることを特徴とする情報記録媒体。

【請求項２２】　コンピュータを請求項１ないし１６のいずれかに記載の情報処理装置として機能させることを特徴とするコンピュータプログラム。

【請求項２３】　情報を再生又は実行するための情報処理方法であって、

前記情報を取得する取得工程と、

前記取得工程において取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているか否かを判定する暗号化判定工程と、

前記暗号化判定工程における判定の結果、前記取得工程において取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときには、前記取得工程における情報の少なくとも一部のさらなる取得を阻止する旨の制御命令、又は前記取得工程において取得された情報の少なくとも一部につき、実行処理を行わず、再生処理を行わず若しくは再生・実行された情報の出力を行わない旨の制御指令を発する制御工程と、

前記取得手段において取得された情報の再生処理又は実行処理を行い、これに

より再生又は実行された情報を出力する処理工程とを備え、

前記制御工程において前記制御指令が発せられたときには、前記取得工程において情報の少なくとも一部のさらなる取得を行わず、又は前記処理工程において実行処理を行わず、再生処理を行わず若しくは再生・実行された情報の出力を行わないことを特徴とする情報処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、例えばコンピュータプログラム、ゲームプログラム、画像情報、音声情報等の情報を再生し又は実行する情報処理装置及び情報処理方法、このような情報を情報記録媒体に記録する情報記録装置、このような情報を記録した情報記録媒体、並びに上記情報処理装置を実現するためのコンピュータプログラムに関する。

【０００２】

【従来の技術】

現在では、画像、音声等の情報が、デジタル情報として、ディスク等の情報記録媒体に記録され、又は通信ネットワークを介して広く流通し、拡散するようになった。また、パーソナルコンピュータ等の普及により、画像、音声等のデータだけでなく、コンピュータプログラムやゲームプログラムといった情報のコピーを容易に作り出すことができるようになった。さらに、これら情報の経済的価値が増し、これら情報に関する著作権その他の財産権の保護を強化する要請が高まった。

【０００３】

このような状況のもと、情報の不法コピーを防止すべく、情報を暗号化する様々な技術が開発されている。また、情報に当該情報が真正なものであることを示す認証情報を付加し、この認証情報に基づいて不法にコピーされた情報の再生又は実行を制限する技術が開発されている。

【０００４】

例えば、映画又は音楽のコンテンツの不法コピーを防止する技術としては、Ｃ

ＳＳ（コンテント・スクランブル・システム）又はＣＰＰＭ（コンテント・プロテクション・フォー・プリレコーディッド・メディア）等が普及している（なお、ＣＳＳについては、例えば、下記の非特許文献１参照）。

【０００５】

また、コンピュータプログラム又はゲームプログラムのコンテンツの不法コピーを防止する技術としては、これらの情報を記録したＲＯＭディスク等の情報記録媒体に認証情報を刻印する技術が普及している。例えば、コンピュータプログラム又はゲームプログラムを記録したＲＯＭディスクの最内周領域に、ロゴ、バーコード等、個性を有する刻印を施す。この刻印が施された領域は、通常の情報記録領域よりもさらに内周側に位置する領域（すなわちディスクの通常の使用形態では非記録領域）であるため、通常の再生装置では、ピックアップをその領域まで移動させることができず、その領域にアクセスすることができない。そこで、ピックアップをその最内周領域まで移動させ、その領域へのアクセスを可能とする特別の機能を、再生装置に付加する。そして、ＲＯＭディスクを再生するときには、その再生装置によって最内周領域にアクセスし、刻印が正しく検出することができない場合には、ＲＯＭディスクの再生を行わないようにする。かかる技術によれば、不法にコピーされたコンピュータプログラム等が記録されたディスクには、その最内周領域に刻印が存在しないので、このようなディスクが再生されるのを防止することができ、これにより、不法コピーの抑制を図ることができる。

【０００６】

【非特許文献１】

館林誠、外３名、「ＤＶＤ著作権保護システム」、映像情報メディア学会技術報告、１９９７年５月２２日、第２１巻、第３１号、ｐ．１５－１９

【０００７】

【発明が解決しようとする課題】

ところが、上述したＣＳＳ及びＣＰＰＭといった暗号化技術は、保護すべき情報に対して、所定の鍵を用い、かつ所定のアルゴリズムに従って情報処理又は演算処理を行うものである。このため、鍵とアルゴリズムが知られてしまえば、暗

号化を解くことができる。もちろん、鍵やアルゴリズムは、情報又はディスクの製作者や提供者、又は著作権保護団体等により秘密に管理されており、一般人が知ることはできない。また、仮に鍵やアルゴリズムに関する情報が漏洩したとしても、暗号化を解くためには、複数の鍵が必要であり、また、アルゴリズムも複雑であるため、暗号化を解くことはきわめて困難である。しかし、これらの暗号化技術は、基本的には情報処理又は演算処理のみに依拠し、物理的・有体的な構造に依拠していないため、高度の情報処理知識を有する技術者により、暗号化が解かれてしまう危険がある。

【０００８】

一方、ＲＯＭディスクの最内周領域に認証情報を刻印する技術は、刻印を用いることや、ピックアップを特別な最内周領域に移動させる機能を再生装置に付加することなど、物理的・有体的な構造に依拠している。したがって、かかる点に着目すれば、情報の保護を強化できるとも思える。しかし、ディスクの最内周領域に存在する刻印を検出する機能（以下、これを「刻印検出機能」という。）は、再生装置に付加された付随的な機能であり、再生装置の通常の情報再生機能とは切り離された独立の機能である。このため、再生装置の一部を改造することによって、刻印検出機能が除去されてしまう危険がある。

【０００９】

また、ＲＯＭディスクの最内周領域などの特別な領域に特別な情報を刻印する方法では、再生装置に特別の機能（例えばピックアップを特別な領域まで移動させる機能など）を付加しなければならない。さらに、ＲＯＭディスクに刻印を形成するためには、専用のディスク製造装置が必要になる。このため、再生装置及びディスクの製造コストが上昇する。

【００１０】

本発明は上記に例示したような問題点に鑑みなされたものであり、本発明の第１の課題は、不法コピー等に対する情報の保護を強化することができる情報処理装置、情報記録装置、情報記録媒体、コンピュータプログラム及び情報処理方法を提供することにある。

【００１１】

本発明の第２の課題は、不法コピー等に対する情報の保護を低コストに実現することができる情報処理装置、情報記録装置、情報記録媒体、コンピュータプログラム及び情報処理方法を提供することにある。

【００１２】

【課題を解決するための手段】

上記課題を解決するために請求項１に記載の情報処理装置は、情報を再生又は実行するための情報処理装置であって、前記情報を取得する取得手段と、前記取得手段により取得された情報の再生処理又は実行処理を行う処理手段と、前記取得手段により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているか否かを判定する暗号化判定手段と、前記暗号化判定手段による判定の結果、前記取得手段により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときには、前記取得手段による情報の少なくとも一部のさらなる取得を阻止するように前記取得手段を制御し、又は前記取得手段により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように前記処理手段を制御する第１制御手段とを備えている。

【００１３】

上記課題を解決するために請求項１７に記載のゲーム装置は、請求項１ないし１６のいずれかに記載の情報処理装置を備えている。

【００１４】

上記課題を解決するために請求項１８に記載の情報記録装置は、情報記録媒体上にコンテンツ情報と前記コンテンツ情報が真正なものであることを示すための認証情報とを記録する情報記録装置であって、前記コンテンツ情報を記録すべき前記情報記録媒体上のアドレスを取得するアドレス取得手段と、前記アドレス取得手段により取得された前記コンテンツ情報のアドレスを用いて所定の演算を行い、当該演算により得られた値を前記認証情報の前記情報記録媒体上のアドレスの値に設定するアドレス設定手段と、前記認証情報を所定の暗号化方式により暗号化する暗号化手段と、前記アドレス取得手段により取得されたアドレスに前記コンテンツ情報を記録し、前記アドレス設定手段により設定されたアドレスに前記暗号化手段により暗号化された認証情報を記録する記録手段とを備えている。

【００１５】

上記課題を解決するために請求項１９に記載の情報記録装置は、多層情報記録媒体上にコンテンツ情報と前記コンテンツ情報が真正なものであることを示すための認証情報とを記録する情報記録装置であって、前記コンテンツ情報を前記多層情報記録媒体のいずれかの層に記録する第１記録手段と前記認証情報を所定の暗号化方式により暗号化する暗号化手段と、前記暗号化手段により暗号化された認証情報を前記多層情報記録媒体の層のうち、前記コンテンツ情報を記録する層以外のいずれかの層に記録する第２記録手段とを備えている。

【００１６】

上記課題を解決するために請求項２０に記載の情報記録媒体は、コンテンツ情報と前記コンテンツ情報が真正なものであることを示すための認証情報とが記録されたコンピュータ読取可能な情報記録媒体であって、前記認証情報は所定の暗号化方式により暗号化された状態で記録されており、前記認証情報の記録アドレスには、前記コンテンツ情報の記録アドレスを用いて所定の演算を行うことによって得られた値が設定されている。

【００１７】

上記課題を解決するために請求項２１に記載の情報記録媒体は、コンテンツ情報と前記コンテンツ情報が真正なものであることを示すための認証情報とが記録されたコンピュータ読取可能な多層情報記録媒体であって、前記コンテンツ情報は前記多層情報記録媒体のいずれかの層に記録されており、前記認証情報は、所定の暗号化方式で暗号化された状態で、前記多層情報記録媒体の層のうち前記コンテンツ情報を記録する層以外のいずれかの層に記録されている。

【００１８】

上記課題を解決するために請求項２２に記載のコンピュータプログラムは、コンピュータを請求項１ないし１６のいずれかに記載の情報処理装置として機能させるものである。

【００１９】

上記課題を解決するために請求項２３に記載の情報処理方法は、情報を再生又は実行するための情報処理方法であって、前記情報を取得する取得工程と、前記

取得工程において取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているか否かを判定する暗号化判定工程と、前記暗号化判定工程における判定の結果、前記取得工程において取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときには、前記取得工程における情報の少なくとも一部のさらなる取得を阻止する旨の制御命令、又は前記取得工程において取得された情報の少なくとも一部につき、実行処理を行わず、再生処理を行わず若しくは再生・実行された情報の出力を行わない旨の制御指令を発する制御工程と、前記取得手段において取得された情報の再生処理又は実行処理を行い、これにより再生又は実行された情報を出力する処理工程とを備え、前記制御工程において前記制御指令が発せられたときには、前記取得工程において情報の少なくとも一部のさらなる取得を行わず、又は前記処理工程において実行処理を行わず、再生処理を行わず若しくは再生・実行された情報の出力を行わない。

【００２０】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて説明する。

【００２１】

（情報処理装置の第１実施形態）

本発明に係る情報処理装置の第１実施形態（以下、これを「第１情報処理装置」という。）について図１を参照して説明する。図１は第１情報処理装置の構成を示している。なお、図１は、本発明の実施形態に係る構成要素等を、その技術思想を説明する限りにおいて具体化したものであり、各構成要素等の形状、位置、接続関係などは、これに限定されるものではない。このことは、以下、本発明の実施形態の説明に用いる図２ないし図９についても同様である。

【００２２】

図１に示す第１情報処理装置１０は、情報を再生又は実行するための装置である。第１情報処理装置１０は、例えば、家庭用ゲーム装置、シミュレーション装置、画像再生装置、音声再生装置等に適用することができ、また、汎用のコンピュータによって実現することも可能である。第１情報処理装置１０の再生又は実行の対象となる情報は、コンピュータプログラム、ゲームプログラム、シミュレ

ーションプログラム、画像情報、音声情報などであり、特に限定されない。

【００２３】

第１情報処理装置１０は、情報を取得する取得手段１１と、取得手段１１により取得された情報の再生処理又は実行処理を行う処理手段１２と、取得手段１１により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているか否かを判定する暗号化判定手段１３と、暗号化判定手段１３による判定の結果、取得手段１１により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときには、取得手段１１による情報の少なくとも一部のさらなる取得を阻止するように取得手段１１を制御し、又は取得手段１１により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように処理手段１２を制御する第１制御手段１４とを備えている。

【００２４】

取得手段１１は、ディスク等の情報記録媒体から情報を取得する場合には、通常、ディスクドライブ等である。例えば、情報記録媒体がＤＶＤ－ＲＯＭである場合には、取得手段１１はＤＶＤ－ＲＯＭドライブである。一方、通信ネットワーク等から情報を取得する場合には、取得手段１１は、例えばネットワークインタフェース等である。このように、取得手段１１は、情報の取得方法等に応じて適宜選択することができ、特に限定されない。

【００２５】

処理手段１２は、コンピュータプログラムに対して実行処理を行う場合には、演算機能及び記憶機能等を備えたプロセッシングユニットである。また、画像情報又は音声情報に対して再生処理を行う場合には、デコード機能等を備えたプロセッシングユニット又はデコードモジュール等である。例えば、再生すべき情報がＭＰＥＧ圧縮された画像情報である場合には、処理手段１２はＭＰＥＧデコードモジュールである。これらのユニットやモジュールは、専用の回路として実現することも可能であるが、汎用のＣＰＵ（セントラルプロセッシングユニット）にソフトウェアを実行させることによって実現することもできる。このように、処理手段１２は、情報の性質・種類、設計・製造上の都合等に応じて適宜選択することができ、特に限定されない。

【００２６】

暗号化判定手段１３は、取得手段１１により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているか否かを判定する手段であり、例えば、演算機能及び記憶機能を有するＣＰＵその他のプロセッシングユニット等により実現することができる。取得手段１１により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているか否かの判定は、情報に付された名前（特に拡張子）を調べる方法、情報が記録された情報記録媒体のファイルシステム情報中のフラグを調べる方法、暗号化された情報自体の性質を調べる方法などが考えられるが、いずれの方法を採用してもよい。

【００２７】

第１制御手段１４は、暗号化判定手段１３による判定の結果、取得手段１１により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときに、取得手段１１による情報の少なくとも一部のさらなる取得を阻止するように取得手段１１を制御し、又は取得手段１１により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように処理手段１２を制御する。例えば、第１情報処理装置１０の実行の対象となる情報がゲームプログラムの場合には、ゲームプログラムのうちの少なくとも一部のさらなる取得を阻止するように取得手段１１を制御し、又は取得手段１１により取得されたゲームプロラムの少なくとも一部を実行せず若しくは最終的に出力しないように処理手段１２を制御する。また、第１情報処理装置１０の再生の対象となる情報が映画や音楽等の画像情報や音声情報の場合には、画像情報や音声情報のうちの少なくとも一部のさらなる取得を阻止するように取得手段１１を制御し、又は取得手段１１により取得された画像情報や音声情報のうちの少なくとも一部を再生せず若しくは最終的に出力しないように処理手段１２を制御する。例えば、取得手段１１により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときには、第１制御手段１４から取得手段１１へ、さらなる情報の取得を中止する旨の指令を送る構成としてもよく、また、第１制御手段１４から処理手段１２へ、情報の少なくとも一部の再生処理又は実行処理を中止し又は開始しない旨の指令を送る構成としてもよい。さらには、第１制御手段１４

から処理手段１２へ、情報の少なくとも一部につき、再生処理後又は実行処理後の出力を中止する旨の指令を送る構成としてもよい。

【００２８】

また、かかる指令に基づいて、再生又は実行の対象となる情報の全部について実行せず、再生せず、又は出力しない構成としてもよいし、当該情報のうち、コピー制限がかけられた情報のみ又は保護の対象となる情報のみについて、取得せず、実行せず、再生せず、又は出力しない構成としてもよい。また、所定の暗号化方式としては、例えば、ＣＳＳ方式、ＣＰＰＭ方式等を用いることができるが、特に限定されない。かかる構成を有する第１制御手段１４は、例えば、演算機能及び記憶機能を有するＣＰＵその他のプロセッシングユニット等により実現することができる。

【００２９】

このような構成を有する第１情報処理装置１０は、以下に示すように動作する。情報を製作又は提供する適法な権限を有する者は、情報を製作又は提供するときに、コンピュータプログラム、ゲームプログラム、映画データ、音楽データ等のコンテンツ情報に、所定の暗号化方式により暗号化された認証情報を付加する。なお、コンテンツ情報に所定の暗号化方式により暗号化された認証情報を付加するのではなく、コンテンツ情報自体を所定の暗号化方式で暗号化してもよい。第１情報処理装置１０の取得手段１１が情報を取得し、その情報の中に所定の暗号化方式により暗号化された認証情報又は所定の暗号化方式により暗号化されたコンテンツ情報が含まれているときには、処理手段１２は、主としてコンテンツ情報に対し、再生処理又は実行処理を行う。なお、このとき、取得手段１１により取得された情報がさらに他の１つ又はいくつかの条件を満たしている場合に限り、取得手段１１が情報の取得を継続し、又は処理手段１２が再生処理若しくは実行処理を行うようにしてもよい。

【００３０】

一方、取得手段１１により取得された情報の中に、所定の暗号化方式により暗号化された情報が含まれていないときには、暗号化判定手段１３はその旨を判定し、第１制御手段１４は、少なくともコンテンツ情報がこれ以上取得手段１１に

よって取得されないように取得手段１１を制御し、又は少なくともコンテンツ情報を再生せず、実行せず若しくは最終的に出力しないように処理手段１２を制御する。この結果、取得手段１１又は処理手段１２は第１制御手段１４の制御に従って動作し、これにより、少なくともコンテンツ情報は再生されず、実行されず又は出力されない。したがって、所定の暗号化方式で暗号化された認証情報が付加されておらず、コンテンツ情報自体も所定の暗号化方式で暗号化されていない場合には、そのコンテンツ情報は第１情報処理装置１０により実行されず、再生されず又は出力されない。

【００３１】

このような第１情報処理装置１０によれば、取得手段１１により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときには、情報の少なくとも一部のさらなる取得を阻止し、又は情報の少なくとも一部を再生せず、実行せず又は出力しない構成としたから、不法コピー等に対する情報の保護を強化することができる。すなわち、情報を製作又は提供する適法な権限を有する者は、情報を製作又は提供するときに、コンテンツ情報に所定の暗号化方式により暗号化された認証情報を付加するか、又はコンテンツ情報自体を所定の暗号化方式で暗号化する。この結果、流通に付される真正の情報は、常に、所定の暗号化方式により暗号化された情報を含んでいることになる。例えば、所定の暗号化方式で暗号化された認証情報が付加されたゲームプログラム（ゲームプログラム自体は暗号化されていない）が記録されたオリジナルディスクを手に入れた者が、ゲームプログラムのコピーディスクを作り出そうと企てているとする。この場合、この者は、オリジナルディスクからゲームプログラムのみを抜き出してブランクディスクにコピーするかもしれない。ところが、このようなコピーディスクを作り出したとしても、このコピーディスクに記録されたゲームプログラムを第１情報処理装置１０で実行（又は最終的に外部へ出力）することはできない。なぜなら、コピーディスクに記録された情報の中には、所定の暗号化方式で暗号化された情報が存在しないからである。

【００３２】

一方、所定の暗号化方式で暗号化された映画データのみが記録されたオリジナ

ルディスクを手に入れた者が、映画データのコピーディスクを作り出そうと企てているとする。この場合、この者は、映画データを見ることができる状態でコピーすることを望むのが通常であるから、映画データの暗号化を解き、暗号化の解かれた状態の映画データをコピーしようとする。ところが、仮にこのような不法コピーを実現することができたとしても、コピーされた映画データを第１情報処理装置１０で再生（又は最終的に外部へ出力）することができない。なぜなら、コピーされた映画データは、もはや所定の暗号化方式で暗号化されていないからである。

【００３３】

また、不法コピーをしようとする者が、情報の暗号化を解いた後、当該情報をさらに所定の暗号化方式で暗号化し、この再度暗号化された状態の情報をコピーすることも考えられる。しかし、情報の暗号化を解くことができたとしても、その情報を再び所定の暗号化方式で暗号化することは、暗号化を解くことに比べて、より一層困難である。例えば、所定の暗号化方式がＣＳＳ方式である場合、タイトル鍵、ディスク鍵、マスタ鍵の３つの鍵を用いた多重の暗号化が行われるため、暗号化を再現するためには、３つの鍵の情報をすべて知らなければならない。また、仮に３つの鍵の情報をすべて知り得たとしても、以下の理由により、暗号化の再現はほとんど不可能である。例えば、ＣＳＳ方式で暗号化した情報を一般に市販されているブランクのＤＶＤ－Ｒに記録する場合を例に挙げると、ＣＳＳ方式の暗号化の過程では、ディスク鍵がマスタ鍵により暗号化された後、ＤＶＤ－Ｒのリードイン領域に書き込まれる。ところが、市販のブランクＤＶＤ－Ｒのリードイン領域には、ブランクディスク用の鍵情報が予め記録されているので、その場所に新たな鍵情報を書き込むことができない。したがって、たとえ３つの鍵の情報をすべて知り得たとしても、暗号化を再現することは、物理的・有体的にみて不可能に等しい。このように、所定の暗号化方式で暗号化された情報のコピーを作り出すことができない以上、第１情報処理装置１０で再生、実行又は出力可能な情報のコピーを作り出すことはできない。

【００３４】

また、不法コピーをしようとする者は、ディスクに所定の暗号化方式で暗号化

されて記録された情報をセクタごとにそのまま他のディスクに転写することによってコピーディスクを作り出そうとするかもしれない。しかし、例えば、所定の暗号化方式がＣＳＳ方式である場合には、オリジナルディスクのリードイン領域に鍵情報が書き込まれている以上、このような方法でコピーディスクを作り出すことはほとんど不可能である。なぜなら、リードイン領域は、通常の一般人が任意にアクセスすることはできない領域であるし、仮に特別な読取装置を用いてリードイン領域から鍵情報を読み取ったとしても、上述したようにこれをブランクのＤＶＤ－Ｒのリードイン領域に転写することはできないからである。このように、所定の暗号化方式で暗号化された情報のコピーを作り出すことができない以上、第１情報処理装置１０で再生、実行又は出力可能な情報のコピーを作り出すことはできない。

【００３５】

以上のように、第１情報処理装置１０により再生、実行又は出力可能な情報のコピーを作り出すことがほとんど不可能であり、この結果、不法コピー等に対する情報の保護を強化することができる。

【００３６】

さらに、第１情報処理装置１０によれば、取得手段１１により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときには、情報の少なくとも一部のさらなる取得を阻止し、又は情報の少なくとも一部を再生せず、実行せず若しくは出力しない構成としたから、不法コピー等に対する情報の保護を低コストで実現することができる。すなわち、情報を所定の暗号化方式で暗号化するのに、専用の工作機械等は不要であり、ただ、所定の暗号化方式で情報を暗号化するためのソフトウェアを用意すれば足りる。したがって、不法コピー等に対する情報の保護を低コストで実現することができる。

【００３７】

なお、コンテンツ情報に所定の暗号化方式により暗号化された認証情報を付する場合、認証情報は、コンテンツ情報が真正なものであることを示すことのできる情報であれば何でもよいのであるが、認証情報を、画像又は音声を含む情報により構成すれば、画像用又は音声用の暗号化方式で認証情報を暗号化することが

できるので便利である。例えば、この場合には、認証情報を暗号化する暗号化方式として、ＣＳＳ方式又はＣＰＰＭ方式等の一般に普及している暗号化方式を用いることができ、コンテンツ情報の保護を低コストに実現することができる。

【００３８】

また、認証情報に情報製作業者又はディスク製作業者等のロゴを表した画像情報を含める構成としてもよい。この場合、当該認証情報に含まれるロゴを、当該認証情報を付加したコンテンツ情報の再生又は実行時に表示するなどして、当該ロゴを商標等として使用する態様を実現すれば、不法コピーを事業として行っている組織等に対する法的責任追及の手段が増え、コンテンツ情報の保護を強化することができる。

【００３９】

（情報処理装置の第２実施形態）

本発明に係る情報処理装置の第２実施形態（以下、これを「第２情報処理装置」という。）について図２を参照して説明する。図２は第２情報処理装置の構成を示している。

【００４０】

図２に示すように、第２情報処理装置２０は、第１情報処理装置１０と同様に、取得手段１１、処理手段１２、暗号化判定手段１３及び第１制御手段１４を備えている。これに加え、第２情報処理装置２０は、取得手段１１により取得された情報の中に所定のフォーマットを有する情報が含まれているか否かを判定するフォーマット判定手段２１と、フォーマット判定手段２１による判定の結果、取得手段１１により取得された情報の中に前記所定のフォーマットを有する情報が含まれていないときには、取得手段１１による情報の少なくとも一部のさらなる取得を阻止するように取得手段１１を制御し、又は取得手段１１により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように処理手段１２を制御する第２制御手段２２とを備えている。

【００４１】

フォーマット判定手段３１は、取得手段１１により取得された情報の中に所定のフォーマットを有する情報が含まれているか否かを判定する手段であり、例え

ば、ＣＰＵその他のプロセッシングユニット等により実現することができる。取得手段１１により取得された情報の中に所定のフォーマットを有する情報が含まれているか否かの判定は、例えば、情報に付された名前（特に拡張子）を調べる方法でもよいし、情報のフォーマットの特性を調べる方法でもよいし、情報が記録された情報記録媒体のファイルシステム情報中のテーブルを調べる方法等でもよい。

【００４２】

第２制御手段３２は、フォーマット判定手段３１による判定の結果、取得手段１１により取得された情報が所定のフォーマットを有していないときに、取得手段１１による情報の少なくとも一部のさらなる取得を阻止するように取得手段１１を制御し、又は取得手段１１により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように処理手段１２を制御する手段であり、例えば、ＣＰＵその他のプロセッシングユニット等により実現することができる。例えば、取得手段１１により取得された情報が所定のフォーマットを有していないときには、第２制御手段２２から取得手段１１へ、情報の少なくとも一部につき、これ以上の取得を中止する旨の指令を送る構成としてもよいし、第２制御手段２２から処理手段１２へ、情報の少なくとも一部につき再生処理又は実行処理を中止し又は開始しない旨の指令を送る構成としてもよい。さらには、第２制御手段２２から処理手段１２へ、情報の少なくとも一部につき、再生処理後又は実行処理後の出力を中止する旨の指令を送る構成としてもよい。

【００４３】

また、所定のフォーマットは、例えば、コンテンツ情報又は認証情報が主として画像情報である場合にはＤＶＤビデオフォーマットがよい。また、コンテンツ情報又は認証情報が主として音声情報である場合には、ＤＶＤオーディオフォーマットがよい。このように、所定のフォーマットは、コンテンツ情報又は認証情報の種類・性質等に応じて適宜選択すればよく、特に限定されない。

【００４４】

このような構成を有する第２情報処理装置２０は、以下に示すように動作する。情報を製作又は提供する適法な権限を有する者は、情報を製作又は提供すると

きに、コンテンツ情報に、所定のフォーマットを有し、かつ所定の暗号化方式で暗号化された認証情報を付加する。なお、コンテンツ情報自体を、所定のフォーマットで製作し、かつ所定の暗号化方式で暗号化してもよい。第２情報処理装置２０の取得手段１１が情報を取得し、その情報の中に、所定のフォーマットを有しかつ所定の暗号方式により暗号化された認証情報、又は所定のフォーマットを有しかつ所定の暗号化方式で暗号化されたコンテンツ情報が含まれているときには、処理手段１２は、主としてコンテンツ情報に対し、再生処理又は実行処理を行う。

【００４５】

一方、取得手段１１により取得された情報の中に、所定のフォーマットを有する認証情報又は所定のフォーマットを有するコンテンツ情報が含まれていないときには、フォーマット判定手段２１はその旨を判定し、第２制御手段２２は、少なくともコンテンツ情報のこれ以上の取得を阻止するように取得手段１１を制御し、又は少なくともコンテンツ情報を再生せず、実行せず若しくは出力しないように処理手段１２を制御する。この結果、取得手段１１又は処理手段１２は第２制御手段２２の制御に従って動作し、これにより、少なくともコンテンツ情報は再生されず、実行されず又は出力されない。

【００４６】

一方、取得手段１１により取得された情報の中に、所定の暗号化方式により暗号化された認証情報又は所定の暗号化方式で暗号化されたコンテンツ情報が含まれていないときには、暗号化判定手段２１はその旨を判定し、第１制御手段１４は、少なくともコンテンツ情報のこれ以上の取得を阻止するように取得手段１１を制御し、又は少なくともコンテンツ情報を再生せず、実行せず若しくは出力しないように処理手段１２を制御する。この結果、取得手段１１又は処理手段１２は第１制御手段１４の制御に従って動作し、これにより、少なくともコンテンツ情報は再生されず、実行されず又は出力されない。

【００４７】

したがって、取得手段１１により取得された情報の中に、所定のフォーマットを有し、かつ所定の暗号化方式により暗号化された情報が含まれていなければ、

少なくともコンテンツ情報は実行されず、再生されず、又は出力されない。

【００４８】

このように、第２情報処理装置２０によっても、不法コピー等に対する情報の保護を強化することができると共に、情報の保護を低コストで実現することができる。特に、第２情報処理装置２０によれば、所定のフォーマットを有し、かつ所定の暗号化方式で暗号化されている情報が存在していなければ実行されず、再生されず又は出力されないという、二重の条件を設定したことにより、不法コピー等に対する情報の保護をより一層強化することができる。

【００４９】

（情報処理装置の第３実施形態）

本発明に係る情報処理装置の第３実施形態（以下、これを「第３情報処理装置」という。）について図３を参照して説明する。図３は第３情報処理装置の構成を示している。

【００５０】

図３に示すように、第３情報処理装置３０は、第１情報処理装置１０と同様に、取得手段１１、処理手段１２、暗号化判定手段１３及び第１制御手段１４を備えている。これに加え、第３情報処理装置３０は、取得手段１１により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているときに、その所定の暗号化方式により暗号化された情報を復号化する復号化手段３１と、復号化手段３１により復号化された情報が認証情報であるか否かを判定する認証情報判定手段３２と、認証情報判定手段３２による判定の結果、復号化された情報が認証情報でないときには、取得手段１１による情報の少なくとも一部のさらなる取得を阻止するように取得手段１１を制御し、又は取得手段１１により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように処理手段１２を制御する第３制御手段３３とを備えている。

【００５１】

復号化手段３１は、所定の暗号化方式に対応する所定の復号化アルゴリズムを備えたデコードモジュール等を備えており、これは、演算機能及び記憶機能等を備えたプロセッシングユニット等により実現することができる。

【００５２】

認証情報判定手段３２は、復号化手段３１により復号化された情報が認証情報であるか否かを判定する手段であり、演算機能及び記憶機能等を備えたプロセッシングユニット等により実現することができる。復号化された情報が認証情報であるか否かの判定は、例えば、第３情報処理装置に認証情報の特徴、データサイズ、内容、記録位置又は相対アドレス等を示すリファレンス情報を予め記憶させておき、判定時に、復号化された情報とリファレンス情報とを比較することによって行うことができる。また、復号化された情報のチェックサムが所定の値か否かを調べることにより、復号化された情報が認証情報であるか否かを判定する構成としてもよい。

【００５３】

第３制御手段３３は、認証情報判定手段３２による判定の結果、復号化された情報が認証情報でないときには、取得手段１１による情報の少なくとも一部のさらなる取得を阻止するように取得手段１１を制御し、又は取得手段１１により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように処理手段１２を制御する手段であり、これも、演算機能及び記憶機能等を備えたプロセッシングユニット等により実現することができる。例えば、復号化された情報が認証情報でないときには、第３制御手段３３から取得手段１１へ、情報の少なくとも一部につき、これ以上の取得を中止する旨の指令を送る構成としてもよいし、第３制御手段３３から処理手段１２へ、情報の少なくとも一部を再生せず又は実行しない旨の指令を送る構成としてもよい。さらには、第３制御手段３３から処理手段１２へ、再生処理後又は実行処理後の出力を中止する旨の指令を送る構成としてもよい。

【００５４】

このような構成を有する第３情報処理装置３０は、以下に示すように動作する。情報を製作又は提供する適法な権限を有する者は、情報を製作又は提供するときに、コンテンツ情報に、所定の特徴、内容又はデータサイズ等を有し、かつ所定の暗号化方式により暗号化された認証情報を付加する。第３情報処理装置３０の取得手段１１が情報を取得し、その情報の中に、所定の暗号化方式により暗号

化された情報が含まれており、かつその情報を復号化した結果、その情報が所定の特徴、内容又はデータサイズ等を有する認証情報であるときには、処理手段１２は、主としてコンテンツ情報に対し、再生処理又は実行処理を行う。

【００５５】

一方、取得手段１１により取得された情報の中に、所定の暗号化方式により暗号化された情報が含まれているものの、その情報を復号化した結果、その情報が所定の特徴、内容又はデータサイズ等を有する認証情報でないときには、認証情報判定手段３２はその旨を判定し、第３制御手段３３は、少なくともコンテンツ情報のこれ以上の取得を阻止するように取得手段１１を制御し、又は少なくともコンテンツ情報を再生せず、実行せず若しくは出力しないように処理手段１２を制御する。この結果、取得手段１１又は処理手段１２は、第３制御手段３３の制御に従って動作し、これにより、少なくともコンテンツ情報は再生されず、実行されず又は出力されない。

【００５６】

一方、取得手段１１により取得された情報の中に、所定の暗号化方式により暗号化された情報が含まれていないときには、暗号化判定手段２１はその旨を判定し、第１制御手段１４は、少なくともコンテンツ情報のこれ以上の取得を阻止するように取得手段１１を制御し、又は少なくともコンテンツ情報を再生せず、実行せず若しくは出力しないように処理手段１２を制御する。この結果、取得手段１１又は処理手段１２は第１制御手段１４の制御に従って動作し、これにより、少なくともコンテンツ情報は再生されず、実行されず又は出力されない。

【００５７】

したがって、取得手段１１により取得された情報の中に、所定の暗号化方式により暗号化され、かつ所定の特徴、内容又はデータサイズ等を有する認証情報が含まれていなければ、少なくともコンテンツ情報は再生されず、実行されず、又は出力されない。

【００５８】

このように、第３情報処理装置３０によっても、不法コピー等に対する情報の保護を強化することができると共に、情報の保護を低コストで実現することがで

きる。特に、第３情報処理装置３０によれば、所定の暗号化方式により暗号化され、かつ所定の特徴、内容又はデータサイズ等を有する認証情報が存在していなければ、実行せず、再生せず、又は出力しないという、二重の条件を設定したことにより、不法コピー等に対する情報の保護をより一層強化することができる。

【００５９】

（情報処理装置の第４実施形態）

本発明に係る情報処理装置の第４実施形態（以下、これを「第４情報処理装置」という。）について図４を参照して説明する。図４は第４情報処理装置の構成を示している。

【００６０】

図４に示すように、第４情報処理装置４０は、第１情報処理装置１０と同様に、取得手段１１、処理手段１２、暗号化判定手段１３及び第１制御手段１４を備え、さらに、第３情報処理装置３０と同様に、復号化手段３１、認証情報判定手段３２及び第３制御手段３３を備えている。これに加え、第４情報処理装置４０は、復号化手段３１により復号化された情報が認証情報であるときに、この認証情報が情報記録媒体上の所定のアドレスに記録されているか否かを判定するアドレス判定手段４１と、アドレス判定手段４１による判定の結果、認証情報が前記所定のアドレスに記録されていないときには、取得手段１１による情報の少なくとも一部のさらなる取得を阻止するように取得手段１１を制御し、又は取得手段１１により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように処理手段１２を制御する第４制御手段４２とを備えている。

【００６１】

アドレス判定手段４１によるアドレス判定は、例えば第４情報処理装置４０に認証情報を記録すべき所定のアドレスを示すリファレンス情報を予め記憶させておき、判定時にそのリファレンス情報と、実際に検出された認証情報のアドレスとを比較する方法により実現することができる。

【００６２】

このような構成を有する第４情報処理装置４０は、以下のように動作する。情

報を製作又は提供する適法な権限を有する者は、情報を製作又は提供するときに、コンテンツ情報に、所定の特徴、内容又はデータサイズ等を有し、かつ所定の暗号化方式により暗号化された認証情報を付加する。さらに、コンテンツ情報と認証情報とを情報記録媒体に記録するときに、認証情報を情報記録媒体の所定のアドレス上に記録する。第４情報処理装置４０の取得手段１１が情報を取得し、その情報の中に、所定の暗号化方式により暗号化された情報が含まれており、その情報を復号化した結果、その情報が所定の特徴、内容又はデータサイズ等を有する認証情報であり、かつ、その認証情報が情報記録媒体上の所定のアドレス上に記録されているときには、処理手段１２は、主としてコンテンツ情報に対し、再生処理又は実行処理を行う。

【００６３】

一方、（ｉ）取得手段１１により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないとき、（ｉｉ）取得手段１１により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているものの、その情報を復号化した結果、その情報が所定の特徴、内容又はデータサイズ等を有する認証情報でないとき、又は（ｉｉｉ）認証情報が情報記録媒体上の所定のアドレスに記録されていないときには、暗号化判定手段１３、認証情報判定手段３２又はアドレス判定手段４１が上記（ｉ）、（ｉｉ）又は（ｉｉｉ）の事実を判定し、第１制御手段１４、第２制御手段３３又は第４制御手段４２が、少なくともコンテンツ情報のこれ以上の取得を阻止するように取得手段１１を制御し、又は少なくともコンテンツ情報を再生せず、実行せず若しくは出力しないように処理手段１２を制御する。この結果、取得手段１１又は処理手段１２は第１制御手段１４、第２制御手段３３又は第４制御手段４２の制御に従って動作し、これにより、少なくともコンテンツ情報は再生されず、実行されず又は出力されない。したがって、取得手段１１により取得された情報の中に、所定の暗号化方式により暗号化され、所定の特徴、内容又はデータサイズ等を有し、かつ、情報記録媒体上の所定のアドレス上に記録された認証情報が含まれていなければ、少なくともコンテンツ情報は再生されず、実行されず又は出力されない。

【００６４】

このように、第４情報処理装置４０によっても、不法コピー等に対する情報の保護を強化することができると共に、情報の保護を低コストで実現することができる。特に、第４情報処理装置４０によれば、所定の暗号化方式により暗号化され、所定の特徴、内容又はデータサイズ等を有する認証情報が存在し、かつ、その認証情報が情報記録媒体上の所定のアドレス上に記録されていなければ実行せず、再生せず又は出力しないという、三重の条件を設定したことにより、不法コピー等に対する情報の保護をより一層強化することができる。

【００６５】

また、第４情報処理装置４０のアドレス判定手段４１を、以下に示すように構成してもよい。すなわち、情報記録媒体に、コンテンツ情報と認証情報が記録されている場合に、コンテンツ情報の情報記録媒体上のアドレスを用いて所定の演算を行うことによって得られる値を、認証情報の情報記録媒体上のアドレスに設定する。このような前提の下で、アドレス判定手段４１を、コンテンツ情報の情報記録媒体上のアドレスを用いて前記所定の演算を実行する演算手段と、認証情報の情報記録媒体上のアドレスの値が演算手段の演算により得られた値と一致するか否かを比較する比較手段とを有する構成とする。

【００６６】

所定の演算の内容は、コンテンツ情報が異なれば、ほぼ常に演算結果が異なるように構成することが好ましい。また、認証情報の記憶領域がコンテンツ情報の記憶領域と重複しないことや、認証情報の記憶領域が情報記録媒体上の記憶領域に収まるようにすることなどを考慮して、所定の演算の内容を決定する。例えば、コンテンツ情報の記録終了アドレスに、コンテンツ情報のサイズを一定値で割った値を加え、その結果得られる値を、認証情報の記録開始アドレスに設定することとしてもよい。

【００６７】

このような構成によれば、認証情報のアドレスがコンテンツ情報のアドレスに基づいて決定されるので、所定の演算方法を知らない者が認証情報のアドレスを知ることはきわめて困難である。また、コンテンツ情報が変われば認証情報のアドレスが変わるため、認証情報のアドレスを知ることはいっそう困難となる。し

たがって、不法コピー等に対する情報の保護を強化することができる。

【００６８】

（情報処理装置の第５実施形態）

本発明に係る情報処理装置の第５実施形態（以下、これを「第５情報処理装置」という。）について図５を参照して説明する。図５は第５情報処理装置の構成を示している。

【００６９】

図５に示すように、第５情報処理装置５０は、第１情報処理装置１０と同様に、取得手段１１、処理手段１２、暗号化判定手段１３及び第１制御手段１４を備え、さらに、第３情報処理装置３０と同様に、復号化手段３１、認証情報判定手段３２及び第３制御手段３３を備えている。これに加え、第５情報処理装置５０は、復号化手段３１により復号化された情報が認証情報であるときに、この認証情報が多層情報記録媒体の所定の層に記録されているか否かを判定する記録層判定手段５１と、記録層判定手段５１による判定の結果、認証情報が所定の層に記録されていないときには、取得手段１１による情報の少なくとも一部のさらなる取得を阻止するように取得手段１１を制御し、又は取得手段１１により取得された情報の少なくとも一部を再生せず、実行せず若しくは最終的に出力しないように処理手段１２を制御する第５制御手段５２とを備えている。

【００７０】

記録層判定手段５１によるアドレス判定は、例えば第５情報処理装置５０に認証情報を記録すべき所定の層番号等を示すリファレンス情報を予め記憶させておき、判定時にそのリファレンス情報と、実際に検出された認証情報の記録された層番号等を比較する方法等により実現することができる。

【００７１】

このような構成を有する第５情報処理装置５０は、以下のように動作する。情報を製作又は提供する適法な権限を有する者は、情報を製作又は提供するときに、コンテンツ情報に、所定の特徴、内容又はデータサイズ等を有し、かつ所定の暗号化方式により暗号化された認証情報を付加する。さらに、コンテンツ情報と認証情報とを多層情報記録媒体に記録するときに、認証情報を多層情報記録媒体

の所定の層に記録する。この場合、認証情報を記録する層は、コンテンツ情報を記録する層と異なる層に記録することが好ましい。より好ましくは、コンテンツ情報を多層情報記録媒体の第１層（通常最初に再生される層又はアドレスの０番が設定されている層）に記録し、認証情報を第２層以降のいずれかの層に記録する。さらに好ましくは、認証情報を、当該認証情報を記録すべき層に形成された記録領域の中間部分又は後半部分に記録する。

【００７２】

第５情報処理装置５０の取得手段１１が情報を取得し、その情報の中に、所定の暗号化方式により暗号化された情報が含まれており、その情報を復号化した結果、その情報が所定の特徴、内容又はデータサイズ等を有する認証情報であり、かつ、その認証情報が多層情報記録媒体の所定の層に記録されているときには、処理手段１２は、主としてコンテンツ情報に対し、再生処理又は実行処理を行う。

【００７３】

一方、（i）取得手段１１により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないとき、（ii）取得手段１１により取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているものの、その情報を復号化した結果、その情報が所定の特徴、内容又はデータサイズ等を有する認証情報でないとき、又は（iii）認証情報が多層情報記録媒体の所定の層に記録されていないときには、暗号化判定手段１３、認証情報判定手段３２又は記録層判定手段５１が上記（i）、（ii）又は（iii）の事実を判定し、第１制御手段１４、第２制御手段３３又は第５制御手段５２が、少なくともコンテンツ情報のこれ以上の取得を中止するように取得手段１１を制御し、又は少なくともコンテンツ情報を再生せず、実行せず若しくは出力しないように処理手段１２を制御する。この結果、取得手段１１又は処理手段１２は第１制御手段１４、第２制御手段３３又は第４制御手段４２の制御に従って動作し、これにより、少なくともコンテンツ情報は再生されず、実行されず又は出力されない。したがって、取得手段１１により取得された情報の中に、所定の暗号化方式により暗号化され、所定の特徴、内容又はデータサイズ等を有し、かつ、多層情報記録媒体の所定

の層に記録された認証情報が含まれていなければ、少なくともコンテンツ情報は再生されず、実行されず又は出力されない。

【００７４】

このように、第５情報処理装置５０によっても、不法コピー等に対する情報の保護を強化することができると共に、情報の保護を低コストで実現することができる。特に、第５情報処理装置５０によれば、所定の暗号化方式により暗号化され、所定の特徴、内容又はデータサイズ等を有する認証情報が存在し、かつ、その認証情報が情報記録媒体の所定の層に記録されていなければ実行せず、再生せず又は出力しないという、三重の条件を設定したことにより、不法コピー等に対する情報の保護をより一層強化することができる。

【００７５】

さらに、情報を不法にコピーしようとする者が、多層情報記録媒体に記録された情報を、１層の情報記録媒体にコピーしようとする場合には、１の層に記録されたコンテンツ情報のみを１層の情報記録媒体にコピーすることができたとしても、他の層に記録された認証情報はコピーすることができない。なぜなら、コピー先の情報記録媒体は１層であるため、コンテンツ情報を記録してしまえば、認証情報を記録する領域がないからである。確かに、コンテンツ情報のデータサイズが小さければ、認証情報を記録する領域があるかもしれない。しかし、この場合には、コピーした結果、認証情報の記録された層もアドレスも変わってしまうため、第５情報処理装置５０又は第４情報処理装置４０により、少なくともコンテンツ情報が実行又は再生されることはない。

【００７６】

また、コンテンツ情報を多層情報記録媒体の第１層に記録し、認証情報を多層情報記録媒体の第２層以降のいずれかの層に記録すれば、製造時の検査作業等において都合がよい。すなわち、多層情報記録媒体の第１層に記録された情報は、通常、最初に再生されるので、製造時の検査作業等を迅速に行うことができる。

【００７７】

さらに、認証情報を、当該認証情報を記録すべき層に形成された情報記録領域の中間部分又は後半部分に記録すれば、不法コピーをしようとする者に対して、

認証情報を見つけにくくすることができる。

【００７８】

（情報記録装置の第１実施形態）

本発明に係る情報記録装置の第１実施形態（以下、これを「第１情報記録装置」という。）について図６を参照して説明する。図６は第１情報記録装置の構成を示している。

【００７９】

図６に示す第１情報記録装置６０は、情報を製作又は提供する適法な権限を有する者、より具体的には情報記録媒体の製造者が、コンテンツ情報及び認証情報が記録された情報記録媒体を製造するときに用いるのに適した情報記録装置である。

【００８０】

第１情報記録装置６０は、コンテンツ情報を記録すべき情報記録媒体上のアドレスを取得するアドレス取得手段６１と、アドレス取得手段６１により取得されたコンテンツ情報のアドレスを用いて所定の演算を行い、当該演算により得られた値を認証情報の情報記録媒体上のアドレスの値に設定するアドレス設定手段６２と、認証情報を所定の暗号化方式により暗号化する暗号化手段６３と、アドレス取得手段６１により取得されたアドレスにコンテンツ情報を記録し、アドレス設定手段６２により設定されたアドレスに暗号化手段６３により暗号化された認証情報を記録する記録手段６４とを備えている。

【００８１】

アドレス取得手段６１は、コンテンツ情報を記録すべき情報記録媒体上のアドレスを取得する。取得方法は、アドレスを手入力する方法でもよいし、情報記録媒体に記録する種々の情報から演算により求める方法でもよい。

【００８２】

アドレス設定手段６２は、アドレス取得手段６１により取得されたコンテンツ情報のアドレスを用いて所定の演算を行い、当該演算により得られた値を認証情報の情報記録媒体上のアドレスの値に設定する。所定の演算の内容は、コンテンツ情報が異なれば、ほぼ常に演算結果が異なるように構成することが好ましい。

例えば、コンテンツ情報の記録終了アドレスに、コンテンツ情報のサイズを一定値で割った値を加え、その結果得られる値を、認証情報の記録開始アドレスに設定することとしてもよい。

【００８３】

暗号化手段６３は、認証情報を所定の暗号化方式により暗号化する。所定の暗号化方式は、例えば、ＣＳＳ方式、ＣＰＰＭ方式などが考えられるが、認証情報の種類・性質（画像情報か音声情報かなど）に応じて適宜選択すればよく、特に限定されない。

【００８４】

記録手段６４は、コンテンツ情報及び暗号化された認証情報をそれぞれの記録アドレスに記録する。

【００８５】

このような構成を有する第１情報記録装置６０によれば、認証情報のアドレスがコンテンツ情報のアドレスに基づいて決定されるので、所定の演算方法を知らない者が認証情報のアドレスを知ることはきわめて困難である。また、コンテンツ情報が変われば認証情報のアドレスが変わるため、認証情報のアドレスを知ることはいっそう困難となる。したがって、上述した第１ないし第５情報処理装置（特に第４情報処理装置）と組み合わせることにより、不法コピー等に対する情報の保護を強化することができる。

【００８６】

また、認証情報の記録アドレスを、コンテンツ情報の記録されている領域、すなわち通常の情報記録領域内（特別の機能を備えた読取装置又は記録装置等しかアクセスできないようなディスクの最内周側などではなく、通常の読取装置又は記録装置等によりアクセス可能な領域内）に設定すれば、不法コピー等に対する情報の保護強化を低コストで実現することができる。なぜなら、この場合には、通常の読取装置や通常の記録装置ではアクセスすることができない領域にアクセスするための専用の機構が不要となるからである。

【００８７】

（情報記録装置の第２実施形態）

本発明に係る情報記録装置の第２実施形態（以下、これを「第２情報記録装置」という。）について図７を参照して説明する。図７は第１情報記録装置の構成を示している。

【００８８】

図７に示す第２情報記録装置７０は、情報を製作又は提供する適法な権限を有する者、より具体的には情報記録媒体の製造者が、コンテンツ情報及び認証情報が記録された多層情報記録媒体を製造するときに用いるのに適した情報記録装置である。

【００８９】

第２情報記録装置７０は、コンテンツ情報を多層情報記録媒体のいずれかの層に記録する第１記録手段７１と、認証情報を所定の暗号化方式により暗号化する暗号化手段７２と、暗号化手段７２により暗号化された認証情報を多層情報記録媒体の層のうち、コンテンツ情報を記録する層以外のいずれかの層に記録する第２記録手段７３とを備えている。

【００９０】

このような構成を有する第２情報記録装置７０によれば、上述した第１ないし第５情報処理装置（特に第５情報処理装置）と組み合わせることにより、不法コピー等に対して情報の保護を強化することができる。例えば、情報を不法にコピーしようとする者が、多層情報記録媒体に記録された情報を、１層の情報記録媒体にコピーしようとする場合には、１の層に記録されたコンテンツ情報のみを１層の情報記録媒体にコピーすることができたとしても、他の層に記録された認証情報はコピーすることができない。なぜなら、コピー先の情報記録媒体は１層であるため、コンテンツ情報を記録してしまえば、認証情報を記録する領域がないからである。確かに、コンテンツ情報のデータサイズが小さければ、認証情報を記録する領域があるかもしれない。しかし、この場合には、コピーした結果、認証情報の記録された層もアドレスも変わってしまうため、第４情報処理装置又は第５情報処理装置により、少なくともコンテンツ情報が実行又は再生されることはない。

【００９１】

また、コンテンツ情報を第２情報記録媒体の第１層に記録し、認証情報を第２情報記録媒体の第２層以降のいずれかの層に記録すれば、製造時の検査作業等において都合がよい。すなわち、第２情報記録媒体の第１層に記録された情報は、通常、最初に再生されるので、製造時の検査作業等を迅速に行うことができる。

【００９２】

また、認証情報を、通常の情報記録領域内（多層情報記録媒体用の通常の読取装置又は記録装置等によりアクセス可能な領域内）に設定すれば、不法コピー等に対する情報の保護強化を低コストで実現することができる。

【００９３】

また、認証情報を、当該認証情報を記録すべき層に形成された情報記録領域内の中間部分又は後半部分に記録すれば、不法コピーをしようとする者に対して、認証情報を見つけにくくすることができる。

【００９４】

（情報記録媒体の第１実施形態）

本発明に係る情報記録媒体の第１実施形態（以下、これを「第１情報記録媒体」という。）について図８を参照して説明する。図８は第１情報記録媒体の情報記録構造を示している。図８中の左側から右側にかけて第１情報記録媒体の記録アドレス値が増加するように設定されている。例えば、第１情報記録媒体がＤＶＤである場合には、図８中の左側がディスクの内周側であり、右側がディスクの外周側である。

【００９５】

図８に示すように、第１情報記録媒体８０は、コンテンツ情報８１とこのコンテンツ情報８１が真正なものであることを示すための認証情報８２とが記録されたコンピュータ読取可能な情報記録媒体であって、認証情報８２は所定の暗号化方式により暗号化された状態で記録されており、認証情報８２の記録アドレスには、コンテンツ情報８１の記録アドレスを用いて所定の演算を行うことによって得られた値が設定されている。

【００９６】

所定の演算の内容は、コンテンツ情報８１が異なれば、ほぼ常に演算結果が異

なるように構成することが好ましい。例えば、コンテンツ情報８１の記録終了アドレスに、コンテンツ情報８１のサイズを一定値で割った値を加え、その結果得られる値を、認証情報８２の記録開始アドレスに設定することとしてもよい。

【００９７】

このような情報記録構造を有する第１情報記録媒体８０によれば、認証情報８２のアドレスがコンテンツ情報８１のアドレスに基づいて決定されるので、所定の演算方法を知らない者が認証情報８２のアドレスを知ることはきわめて困難である。また、コンテンツ情報８１が変われば認証情報８２のアドレスが変わるため、認証情報８２のアドレスを知ることはいっそう困難となる。したがって、上述した第１ないし第５情報処理装置（特に第４情報処理装置）と組み合わせることにより、不法コピー等に対する情報の保護を強化することができる。

【００９８】

また、認証情報８２の記録アドレスを、コンテンツ情報８１の記録されている領域、すなわち通常の情報記録領域内（特別の機能を備えた読取装置又は記録装置等しかアクセスできないようなディスクの最内周側などではなく、通常の読取装置又は記録装置等によりアクセス可能な領域内）に設定すれば、不法コピー等に対する情報の保護強化を低コストで実現することができる。なぜなら、この場合には、通常の読取装置や通常の記録装置ではアクセスすることができない領域にアクセスするための専用の機構が不要となるからである。

【００９９】

（情報記録媒体の第２実施形態）

本発明に係る情報記録媒体の第２実施形態（以下、これを「第２情報記録媒体」という。）について図９を参照して説明する。図９は第１情報記録媒体の情報記録構造を示している。なお、図９は、第２情報記録媒体９０の具体例として、層Ｌ１及び層Ｌ２の２層の情報記録媒体を例示しているが、３層以上の情報記録媒体でもよい。

【０１００】

図９に示すように、第２情報記録媒体９０は、コンテンツ情報９１とこのコンテンツ情報９１が真正なものであることを示すための認証情報９２とが記録され

たコンピュータ読取可能な多層情報記録媒体であって、コンテンツ情報９１は第２情報記録媒体９０のいずれかの層（例えば層Ｌ１）に記録されており、認証情報９２は、所定の暗号化方式で暗号化された状態で、第２情報記録媒体９０の層のうちコンテンツ情報９１を記録する層以外のいずれかの層（例えば層Ｌ２）に記録されている。

【０１０１】

このような情報記録構造を有する第２情報記録媒体９０によれば、上述した第１ないし第５情報処理装置（特に第５情報処理装置）と組み合わせることにより、不法コピー等に対して情報の保護を強化することができる。例えば、情報を不法にコピーしようとする者が、第２情報記録媒体９０に記録された情報を、１層の情報記録媒体にコピーしようとする場合には、１の層（Ｌ１）に記録されたコンテンツ情報９１のみを１層の情報記録媒体にコピーすることができたとしても、他の層（Ｌ２）に記録された認証情報９２はコピーすることができない。なぜなら、コピー先の情報記録媒体は１層であるため、コンテンツ情報９１を記録してしまえば、認証情報９２を記録する領域がないからである。確かに、コンテンツ情報９１のデータサイズが小さければ、認証情報９２を記録する領域があるかもしれない。しかし、この場合には、コピーした結果、認証情報９２の記録された層もアドレスも変わってしまうため、第４情報処理装置又は第５情報処理装置により、少なくともコンテンツ情報９１が実行又は再生されることはない。

【０１０２】

また、コンテンツ情報９１を第２情報記録媒体９０の第１層に記録し、認証情報９２を第２情報記録媒体９０の第２層以降のいずれかの層に記録すれば、製造時の検査作業等において都合がよい。すなわち、第２情報記録媒体９０の第１層に記録された情報は、通常、最初に再生されるので、製造時の検査作業等を迅速に行うことができる。

【０１０３】

また、認証情報９２を、通常の情報記録領域内（多層情報記録媒体用の通常の読取装置又は記録装置等によりアクセス可能な領域内）に設定すれば、不法コピー等に対する情報の保護強化を低コストで実現することができる。

【０１０４】

また、認証情報９２を、当該認証情報を記録すべき層に形成された情報記録領域内の中間部分又は後半部分に記録すれば、不法コピーをしようとする者に対して、認証情報９２を見つけにくくすることができる。

【０１０５】

（情報処理方法の実施形態）

本発明に係る情報処理方法の実施形態について説明する。本発明の実施形態に係る情報処理方法は、情報を再生又は実行するための情報処理方法であって、情報を取得する取得工程と、取得工程において取得された情報の中に所定の暗号化方式により暗号化された情報が含まれているか否かを判定する暗号化判定工程と、暗号化判定工程における判定の結果、取得工程において取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときには、取得工程における情報の少なくとも一部のさらなる取得を阻止する旨の制御命令、又は取得工程において取得された情報の少なくとも一部につき、実行処理を行わず、再生処理を行わず若しくは再生・実行された情報の出力を行わない旨の制御指令を発する制御工程と、取得手段において取得された情報の再生処理又は実行処理を行い、これにより再生又は実行された情報を出力する処理工程とを備え、制御工程において制御指令が発せられたときには、取得工程において情報の少なくとも一部のさらなる取得を行わず、又は処理工程において実行処理を行わず、再生処理を行わず若しくは再生・実行された情報の出力を行わない。

【０１０６】

より具体的に説明すると、情報を製作又は提供する適法な権限を有する者は、情報を製作又は提供するときに、コンピュータプログラム、ゲームプログラム、映画データ、音楽データ等のコンテンツ情報に、所定の暗号化方式により暗号化された認証情報を付加する。なお、コンテンツ情報に所定の暗号化方式により暗号化された認証情報を付加するのではなく、コンテンツ情報自体を所定の暗号化方式で暗号化してもよい。さて、取得工程において情報を取得し、その情報の中に、所定の暗号化方式により暗号化された認証情報又は所定の暗号化方式により暗号化されたコンテンツ情報が含まれているときには、処理工程において、主と

してコンテンツ情報に対し、再生処理又は実行処理を行う。なお、このとき、取得工程において取得された情報がさらに他の１つ又はいくつかの条件を満たしている場合に限り、処理工程において再生処理又は実行処理を行うようにしてもよい。

【０１０７】

一方、取得工程において取得された情報の中に、所定の暗号化方式により暗号化された情報が含まれていないときには、暗号化判定工程においてその旨を判定し、第１制御工程において、少なくともコンテンツ情報のこれ以上の取得を行わず、又は少なくともコンテンツ情報の実行処理を行わず、再生処理を行わず若しくは再生・実行された情報の出力を行わない旨の制御指令を発する。この結果、取得工程又は処理工程における取得、再生、実行等の処理が、第１制御工程において発せられた制御指令に従って阻止、中止又は無効とされ、これにより、少なくともコンテンツ情報は実行されず、再生されず又は出力されない。したがって、所定の暗号化方式で暗号化されていないコンテンツ情報は再生されず、実行されず、出力されない。

【０１０８】

このような情報処理方法によれば、取得工程において取得された情報の中に所定の暗号化方式により暗号化された情報が含まれていないときには、情報の少なくとも一部につき実行せず、再生せず又は出力しない構成としたから、不法コピー等に対する情報の保護を強化することができると共に、不法コピー等に対する情報の保護を低コストで実現することができる。

【０１０９】

なお、以上のような実施形態は、専用の装置としてハードウェアと一体的に構成する形態で実現してもよいし、コンピュータにプログラムを読み込ませることによって実現してもよい。

【０１１０】

【実施例】

以下、本発明の実施例を図面に基づいて説明する。以下の実施例は、本発明に係る情報処理装置を家庭用ゲーム装置に適用した例である。

【０１１１】

まず、本発明の実施例に係るゲーム装置について図１０を参照して説明する。図１０は本発明の実施例に係るゲーム装置の構成を示している。

【０１１２】

図１０に示すように、ゲーム装置１００は、ＤＶＤ－ＲＯＭ１１０に記録されたゲームプログラムを実行する装置である。ゲーム装置１００は、ＤＶＤ－ＲＯＭドライブ１０１、ＣＰＵ１０２、メモリ１０３及びデコードモジュール１０４を備えており、これらはバス１０５を介して相互に接続されている。また、バス１０５にはゲーム用コントローラ１０６が接続され、デコードモジュール１０４には、ディスプレイ１０７及びスピーカ１０８が接続されている。

【０１１３】

ＤＶＤ－ＲＯＭドライブ１０１は、ゲームプログラム１１２、認証情報１１３等が記録されたＤＶＤ－ＲＯＭ１１０（図１１参照）から、ゲームプログラム１１２、認証情報１１３等を読み取る情報読取装置である。ＤＶＤ－ＲＯＭドライブ１０１は、ＣＳＳに準拠しており、デコードモジュール１０４と共に、ＣＳＳ暗号化された情報の復号化（暗号化の解除）をする機能を備えている。

【０１１４】

ＣＰＵ１０２は、ゲーム装置１００の全体的な制御を行うと共に、ゲームプログラム及び後述する実行許否判定処理等を実行する。

【０１１５】

メモリ１０３は、例えばリードオンリメモリであり、実行許否判定処理プログラムの他、各種プログラム、データを格納している。

【０１１６】

デコードモジュール１０４は、例えばＭＰＥＧデコードモジュールであり、ＭＰＥＧ圧縮された画像情報等をデコードし、再生するモジュールである。デコードモジュール１０４は、デコード回路の他、デジタルーアナログ変換回路等を備えている。さらに、デコードモジュール１０４は、ＣＳＳに準拠しており、ＤＶＤ－ＲＯＭドライブ１０１と共に、ＣＳＳ暗号化された画像情報を復号化する機能を備えている。後述するように、認証情報１１３はＤＶＤビデオフォーマット

を有し、かつＣＳＳ暗号化された画像情報である。デコードモジュール１０４は、この認証情報１１３を復号化してその内容を認識するために用いられる。なお、当該ゲーム装置１００が、ＤＶＤ－ＲＯＭに記録されたゲームプログラムを実行するだけでなく、ＤＶＤビデオディスクに記録された映画等を再生する機能を兼ね備えている場合には、デコードモジュール１０４により、ＤＶＤビデオフォーマットを有し、かつＣＳＳ暗号化された映画データ等を復号化して再生することができる。

【０１１７】

このような構成を有するゲーム装置１００は、以下のように動作する。ユーザがＤＶＤ－ＲＯＭ１１０をＤＶＤ－ＲＯＭドライブ１０１に装着すると、ＤＶＤ－ＲＯＭドライブ１０１は、ＤＶＤ－ＲＯＭドライブ１０１のファイルシステム情報１１１等にアクセスし、続いてＤＶＤ－ＲＯＭ１１０に記録されたゲームプログラム１１２、認証情報１１３等を読み取る。この読取動作とほぼ同時に、ＣＰＵ１０２は、ＤＶＤ－ＲＯＭドライブ１０１及びデコードモジュール１０４と協働して、実行許否判定処理を行う。実行許否判定処理において、ＣＰＵ１０２は、ＤＶＤ－ＲＯＭ１１０に記録されたゲームプログラム１１２等が真正のものか、すなわち不法にコピーされたものでないかを判定する。実行許否判定処理の結果、ゲームプログラム１１２が真正のものであるときには、ＣＰＵ１０２は、ゲームプログラム１１２を実行する。一方、ゲームプログラム１１２が真正のものでないときには、ＣＰＵ１０２は、ゲームプログラム１１２の実行を行わない。

【０１１８】

次に、ＤＶＤ－ＲＯＭ１１０に記録された情報の記録構造について図１１を参照して説明する。図１１はＤＶＤ－ＲＯＭ１１０に記録された情報の記録構造を示している。なお、図１１中の左側がＤＶＤ－ＲＯＭディスクの内周側であり、右側がＤＶＤ－ＲＯＭディスクの外周側である。

【０１１９】

図１１に示すように、ＤＶＤ－ＲＯＭ１１０は、シングルレイヤータイプのＤＶＤ－ＲＯＭディスクであり、その内周側にはリードイン領域Ａ１が形成され、

その外周側にボリューム領域Ａ２が形成され、さらにその外周側にリードアウト領域Ａ３が形成されている。

【０１２０】

ボリューム領域Ａ２は、ＤＶＤ－ＲＯＭディスクに記録された情報を読み取る機能を有する一般ユーザ向けの情報読取装置（ＤＶＤ－ＲＯＭドライブ１０１もこれに含まれる）を通常の操作方法で操作することによって任意にアクセスすることができる通常の情報記録領域である。一方、リードイン領域Ａ１及びリードアウト領域Ａ３は、ＤＶＤ－ＲＯＭディスクに記録された情報を読み取る機能を有する一般ユーザ向けの情報読取装置を通常の操作方法で操作することによって任意にアクセスすることができない情報記録領域である。もっとも、リードイン領域Ａ１及びリードアウト領域Ａ３は、ユーザが任意にアクセスすることができない領域ではあるが、上記一般ユーザ向けの情報読取装置によって全くアクセスすることができない領域ではない。すなわち、当該情報読取装置のピックアップはリードイン領域Ａ１又はリードアウト領域Ａ３まで移動することができ、情報読取装置の内部プログラムによってリードイン領域Ａ１又はリードアウト領域Ａ３のアドレスを指定すれば、それらの領域にアクセスすることができる。なお、ＤＶＤには、リードイン領域のさらに内周側には若干の非記録領域が存在するが、この非記録領域は、上記一般ユーザ向けの情報読取装置によってアクセスすることはできず、この領域にアクセスさせるためには、情報読取装置に特別の機能を付加しなければならない。

【０１２１】

ＤＶＤ－ＲＯＭ１１０のボリューム領域Ａ２内には、その内周側にファイルシステム情報１１１が記録されている。ファイルシステム情報１１１は、ボリューム領域Ａ２内に記録されている情報を管理するための情報であり、これには、このファイルシステム情報１１１に続いてボリューム領域Ａ２内に記録されている個々の情報の名前、記録アドレス、データサイズ、データフォーマット、暗号化の有無等を示す情報が含まれている。

【０１２２】

また、ボリューム領域Ａ２内には、ファイルシステム情報１１１に続いて、ゲ

ームプログラム１１２が記録されている。ゲームプログラム１１２は、例えば対戦ゲーム、シューティングゲーム、野球ゲーム、ロールプレイングゲーム等を実現するためのコンピュータプログラムである。ゲームプログラム１１２は、暗号化されていない状態で記録されている。また、ゲームプログラム１１２は、プログラムなので、ＤＶＤビデオフォーマットではない。なお、ゲームの内容によっては、ゲームプログラムだけでなく、ゲームを再現するための画像情報や音声情報をＤＶＤ－ＲＯＭ１１０に記録することができる。この場合には、画像情報及び音声情報をＤＶＤビデオフォーマット（ＤＶＤオーディオフォーマットでもよい）で記録することができる。また、この場合、画像情報及び音声情報をＣＳＳ暗号化（ＣＰＰＭ暗号化）して記録してもよい。

【０１２３】

さらに、ボリューム領域Ａ２内には、認証情報１１３が記録されている。認証情報１１３は、例えば、ディスク製造業者のロゴを表した画像に対応した画像情報である。認証情報１１３のフォーマットは、ＤＶＤビデオフォーマットである。さらに、認証情報１１３は、情報を製作又は提供する適法な権限を有するディスク製造業者により、当該ＤＶＤ－ＲＯＭディスクを製造する過程で、ＣＳＳ暗号化されて記録されている。

【０１２４】

ＤＶＤ－ＲＯＭ１１０のリードイン領域Ａ１内には、マスタ鍵を用いて暗号化されたディスク鍵が記録されている。この鍵はＣＳＳ暗号化・復号化時に用いられるものである。この暗号化されたディスク鍵は、リードイン領域Ａ１内に記録されているので、ユーザが任意に読み取ることができないが、一般ユーザ向けの情報読取装置の内部的制御にしたがって（内蔵の制御プログラムによって）読み取ることは可能である。

【０１２５】

次に、認証情報１１３の暗号化・復号化に用いられる暗号化方式であるＣＳＳについて説明する。なお、以下のＣＳＳの説明では、いったん実施例に係るゲーム装置１００を離れ、一般的な視点から説明する。

【０１２６】

ＣＳＳは、主として映画ソフトをＤＶＤコンテンツとして提供する場合に、映画ソフトの著作権を保護することを目的として開発された情報暗号化技術であり、周知の技術である。ＤＶＤに記録すべきコンテンツ情報の暗号化は、タイトル鍵、ディスク鍵、マスタ鍵の３つの鍵を用いて行われる。まず、ＤＶＤに記録すべきコンテンツ情報は、圧縮（例えばＭＰＥＧ圧縮）等の処理を経た後、タイトル鍵を用いてスクランブルされる。次に、タイトル鍵は、ディスク鍵を用いて暗号化され、暗号化されたタイトル鍵は、ＤＶＤ上のセクターヘッダ領域に記録される。セクターヘッダ領域は、ユーザが任意にアクセスすることができない領域である。次に、ディスク鍵は、マスタ鍵を用いて暗号化され、暗号化されたディスク鍵は、ＤＶＤ上のリードイン領域に記録される。

【０１２７】

ＤＶＤに暗号化されて記録されたコンテンツ情報を再生装置等によって再生する場合には、再生装置等がＣＳＳ準拠のものでなければならない。ＤＶＤに暗号化されて記録されたコンテンツ情報をＣＳＳ準拠の再生装置等により再生するときには、以下に述べる復号化プロセスが行われる。すなわち、ＣＳＳ準拠の再生装置等は、マスタ鍵を予め秘密に保持している。まず、再生装置等は、ＤＶＤ上のリードイン領域に暗号化されて記録されているディスク鍵を読み取り、これを、自ら秘密に保持しているマスタ鍵を用いて復号化し、取得する。次に、再生装置等は、ＤＶＤ上のセクターヘッダ領域に暗号化されて記録されているタイトル鍵を読み取り、これを、先ほどＤＶＤから取得したディスク鍵を用いて復号化し、取得する。次に、再生装置等は、ＤＶＤ上にスクランブルがかけられた状態で記録されたコンテンツ情報を読み取り、これを、先ほどＤＶＤから取得したタイトル鍵を用いてデスクランブルする。そして、再生装置等は、デスクランブルされたコンテンツ情報を再生する。例えば、コンテンツ情報が圧縮されているデジタル映像であるときには、再生装置等は、内蔵しているデコーダ（例えばＭＰＥＧデコーダ）によって、コンテンツ情報をデコードし、これをデジタルーアナログ変換してディスプレイ等に出力する。

【０１２８】

また、ＤＶＤに暗号化されて記録されているコンテンツ情報を汎用コンピュー

タによって再生するためには、汎用コンピュータが備えているＤＶＤ－ＲＯＭドライブ及びデコードモジュール（例えばＭＰＥＧデコードモジュール）がいずれもＣＳＳ準拠のものでなければならない。ＤＶＤに暗号化されて記録されているコンテンツ情報を、ＣＳＳ準拠のＤＶＤ－ＲＯＭドライブ及びＣＳＳ準拠のデコードモジュールを備えた汎用コンピュータによって再生するときには、上述した復号化プロセスに加えて、以下に述べるパス認証プロセスが行われる。すなわち、ＤＶＤに暗号化されて記録されているコンテンツ情報に対して上述した復号化プロセスを実行する前に、ＤＶＤ－ＲＯＭドライブとデコードモジュールとの間でパス認証が実行される。具体的には、ＤＶＤ－ＲＯＭドライブとデコードモジュールはコンピュータのバスを介して相互に接続されており、このバスを介して両者間で互いにＣＳＳ準拠であることの確認が行われる。このとき、ＤＶＤ－ＲＯＭドライブとデコードモジュールとの間で、両者のみが認識し得る時変鍵が作り出される。その後、ＤＶＤ－ＲＯＭドライブとデコードモジュールとによって、上述した復号化プロセスが実行される。この復号化プロセスの中で、ＤＶＤ－ＲＯＭドライブがデコードモジュールへ、タイトル鍵又はディスク鍵を渡すときには、その鍵は時変鍵により暗号化される。そして、デコードモジュールがＤＶＤ－ＲＯＭドライブから渡された鍵を利用するときには、その鍵は時変鍵を用いて復号化される。

【０１２９】

本実施例に係るゲーム装置１００は、ＣＳＳ準拠のＤＶＤ－ＲＯＭドライブ１０１及びＣＳＳ準拠のデコードモジュール１０４を備えており、ＣＳＳ暗号化されてＤＶＤ－ＲＯＭ１１０に記録された認証情報を復号化することができる。復号化の際には、ＤＶＤ－ＲＯＭ１１０のリードイン領域Ａ１に記録されたディスク鍵１１４が用いられる。

【０１３０】

次に、ゲーム装置１００における実行許否判定処理について図１２を参照して説明する。実行許否判定処理は、ＤＶＤ－ＲＯＭ１１０に記録されたゲームプログラム１１２が真正のものか、すなわち不法にコピーされたものでないかを判定し、その判定結果に基づいて、ゲームプログラム１１２を実行するか実行しない

かの制御を行う処理である。この実行許否判定処理はＣＰＵ１０２の制御のもとで行われる。

【０１３１】

図１２に示すように、ＤＶＤ－ＲＯＭドライブ１０１にＤＶＤ－ＲＯＭ１１０が装着されると（ステップＳ１：ＹＥＳ）、ＣＰＵ１０２は、ＤＶＤ－ＲＯＭ１１０のボリューム領域Ａ２内にＤＶＤビデオフォーマットを有する情報が記録されているか否かを判定する（ステップＳ２）。ファイルシステム情報１１１内には、ボリューム領域Ａ２内に記録されている個々の情報（ファイル）の名前が記述されており、情報の名前には、フォーマットごとに異なる拡張子が付加されている。したがって、ボリューム領域Ａ２内にＤＶＤビデオフォーマットを有する情報が記録されているか否かの判定は、ファイルシステム情報１１１内に記述された情報の拡張子を調べることにより実現することができる。

【０１３２】

ボリューム領域Ａ２内にＤＶＤビデオフォーマットを有する情報が記録されていないときには（ステップＳ２：ＮＯ）、ＣＰＵ１０２は、ゲームプログラム１１２の実行を拒絶するための制御を行う（ステップＳ９）。この結果、ゲームプログラム１１２は実行されない。

【０１３３】

一方、ボリューム領域Ａ２内にＤＶＤビデオフォーマットを有する情報が記録されているときには（ステップＳ２：ＹＥＳ）、ＣＰＵ１０２は、続いて、ＤＶＤビデオフォーマットを有する情報の中に、ＣＳＳ暗号化された情報があるか否かを判定する（ステップＳ３）。ＣＳＳ暗号化された情報があるか否かの判定は、リードイン領域Ａ１に記録されたフラグを調べることによって実現することができる。

【０１３４】

ＤＶＤビデオフォーマットを有する情報の中に、ＣＳＳ暗号化された情報がないときには（ステップＳ３：ＮＯ）、ＣＰＵ１０２は、ゲームプログラム１１２の実行を拒絶するための制御を行う（ステップＳ９）。この結果、ゲームプログラム１１２は実行されない。

【０１３５】

一方、ＤＶＤビデオフォーマットを有する情報の中に、ＣＳＳ暗号化された情報があるときには（ステップＳ３：ＹＥＳ）、ＣＰＵ１０２は、ＤＶＤ－ＲＯＭドライブ１０１及びデコードモジュール１０４と協働して、ＣＳＳ暗号化された情報を復号化する（ステップＳ４）。

【０１３６】

続いて、ＣＰＵ１０２は、復号化された情報が認証情報１１３か否かを判定する（ステップＳ５）。この判定は、復号化された情報のチェックサムの値を求め、これを予めメモリ１０３に記録された基準値と比較することによって行う。復号化された情報のチェックサムの値と基準値とが一致したときに限り、復号化された情報が認証情報１１３であると判定する。

【０１３７】

復号化された情報が認証情報１１３でないときには（ステップＳ５：ＮＯ）、ＣＰＵ１０２は、ゲームプログラム１１２の実行を拒絶するための制御を行う（ステップＳ９）。この結果、ゲームプログラム１１２は実行されない。

【０１３８】

一方、復号化された情報が認証情報１１３であるときには（ステップＳ５：ＹＥＳ）、ＣＰＵ１０２は、続いて、認証情報１１３の基準アドレスを算出する（ステップＳ６）。ディスク製造業者は、ＤＶＤ－ＲＯＭ１１０の製造過程において、ＤＶＤ－ＲＯＭ１１０にゲームプログラム１１２及び認証情報１１３を記録するとき、ゲームプログラム１１２の記録アドレスを用いて所定の演算を行い、その演算の結果得られた値を、認証情報１１３の記録アドレスに設定している。具体的には、ゲームプログラム１１２の記録終了アドレスに、ゲームプログラム１１２のサイズを一定値で割った値を加え、その結果得られる値を、認証情報１１３の記録開始アドレスに設定している。したがって、ＤＶＤ－ＲＯＭ１０１のボリューム領域Ａ２内において、認証情報１１３が記録されているアドレスは、前記所定の演算を行うことによって得ることができる。そこで、ステップＳ６で、ＣＰＵ１０２は、上記所定の演算を行い、その結果得られた値を、基準アドレスとして取得する。

【０１３９】

続いて、ＣＰＵ１０２は、ＤＶＤ－ＲＯＭ１１０に実際に記録されている認証情報１１３の現実の記録開始アドレスを検出し、この現実の記録開始アドレスと基準アドレスとを比較する。このようにして、ＣＰＵ１０２は、現実の記録開始アドレスが基準アドレスに一致するか否かを判定する（ステップＳ７）。

【０１４０】

現実の記録開始アドレスが基準アドレスに一致しないときには（ステップＳ７：ＮＯ）、ＣＰＵ１０２は、ゲームプログラム１１２の実行を拒絶するための制御を行う（ステップＳ９）。この結果、ゲームプログラム１１２は実行されない。

【０１４１】

一方、現実の記録開始アドレスが基準アドレスに一致したときには（ステップＳ７：ＹＥＳ）、ＣＰＵ１０２は、ゲームプログラム１１２の実行を許可するための制御を行う（ステップＳ８）。

【０１４２】

このように、本実施例に係るゲーム装置１００によれば、ＤＶＤビデオフォーマットを有し、ＣＳＳ暗号化され、かつ、所定のチェックサムを有する認証情報１１３が、ＤＶＤ－ＲＯＭ１１０のボリューム領域Ａ２内の所定のアドレスに記録されている場合に限り、ゲームプログラム１１２の実行が許可される。すなわち、（ｉ）ディスク上に認証情報が存在しない場合、（ｉｉ）ディスク上に認証情報が存在していてもそれがＤＶＤビデオフォーマットでない場合、（ｉｉｉ）認証情報がＣＳＳ暗号化されていない場合、又は、（ｉｖ）認証情報が上記所定の演算で算出される所定のアドレスとは異なるアドレスに記録されている場合には、ゲームプログラム１１２は実行されない。したがって、不法コピー等に対して、ゲームプログラム１１２を強力に保護することができる。

【０１４３】

確かに、不法コピーをしようとする者が、一般に市販されているブランクのＤＶＤ－Ｒ等の上に、ＤＶＤ－ＲＯＭ１１０に記録された情報のすべてを全くそのままコピーすれば、このようにして不法コピーされたゲームプログラムは、ゲー

ム装置１００で再生することができてしまう。しかし、これはほとんど不可能である。なぜなら、上述したように、仮に認証情報のＣＳＳ暗号化を解くことができたとしても、それを再びＣＳＳ暗号化することはほとんど不可能であるし、また、ＣＳＳ暗号化された認証情報をセクタごとにそのまま転写してコピーディスクを作り出すことはＣＳＳの構造上ほとんど不可能だからである。

【０１４４】

さらに、本実施例に係るゲーム装置１００によれば、認証情報１１３の正しい記録アドレスが、ゲームプログラム１１２の記録終了アドレス及びサイズに基づいて決定されるので、ゲームプログラム１１２の記録位置又はサイズが異なれば、認証情報１１３の正しい記録アドレスも変化する。このことから、不法なコピーディスクの作成はより一層困難となり、ゲームプログラムの保護をより一層強化することができる。

【０１４５】

さらに、本実施例に係るゲーム装置１００によれば、一般に用いられる情報読取装置又は情報記録装置によって通常にアクセスすることが可能なボリューム領域Ａ２に、認証情報１１３を記録し、その認証情報１１３を検出して所定の判定処理を行うことで、ゲームプログラム１１２の実行の許否を決定することができる。また、一般に広く知られているＣＳＳを認証情報１１３の暗号化方式として採用している。このため、コピープロテクトを実現するのに、専用のディスク製造装置や専用の情報読取装置は不要である。したがって、不法コピー等に対するゲームプログラム１１２の保護を低コストで実現することができる。

【０１４６】

なお、本発明は、請求の範囲および明細書全体から読み取るこのできる発明の要旨または思想に反しない範囲で適宜変更可能であり、そのような変更を伴うゲーム装置、情報処理装置、情報記録装置、情報処理方法及びこれらの機能を実現するコンピュータプログラム並びに情報記録媒体もまた本発明の技術思想に含まれる。

【図面の簡単な説明】

【図１】

本発明に係る情報処理装置の第１実施形態を示すブロック図である。

【図２】

本発明に係る情報処理装置の第２実施形態を示すブロック図である。

【図３】

本発明に係る情報処理装置の第３実施形態を示すブロック図である。

【図４】

本発明に係る情報処理装置の第４実施形態を示すブロック図である。

【図５】

本発明に係る情報処理装置の第５実施形態を示すブロック図である。

【図６】

本発明に係る情報記録装置の第１実施形態を示すブロック図である。

【図７】

本発明に係る情報記録装置の第２実施形態を示すブロック図である。

【図８】

本発明に係る情報記録媒体の第１実施形態を示すブロック図である。

【図９】

本発明に係る情報記録媒体の第２実施形態を示すブロック図である。

【図１０】

本発明の実施例に係るゲーム装置を示すブロック図である。

【図１１】

本発明の実施例に係るＤＶＤ－ＲＯＭを示す説明図である。

【図１２】

本発明の実施例に係る実行許否判定処理を示すフローチャートである。

【符号の説明】

１０、２０、３０、４０、５０…情報処理装置

１１…取得手段

１２…処理手段

１３…暗号化判定手段

１４…第１制御手段

２１…フォーマット判定手段

２２…第２制御手段

３１…復号化手段

３２…認証情報判定手段

３３…第３制御手段

４１…アドレス判定手段

４２…第４制御手段

５１…記録層判定手段

５２…第５制御手段

６０、７０…情報記録装置

６１…アドレス取得手段

６２…アドレス設定手段

６３、７２…暗号化手段

６４…記録手段

７１…第１記録手段

７３…第２記録手段

８０、９０…情報記録媒体

８１、９１…コンテンツ情報

８２、９２、１１３…認証情報

１００…ゲーム装置

１０１…ＤＶＤ－ＲＯＭドライブ

１０２…ＣＰＵ

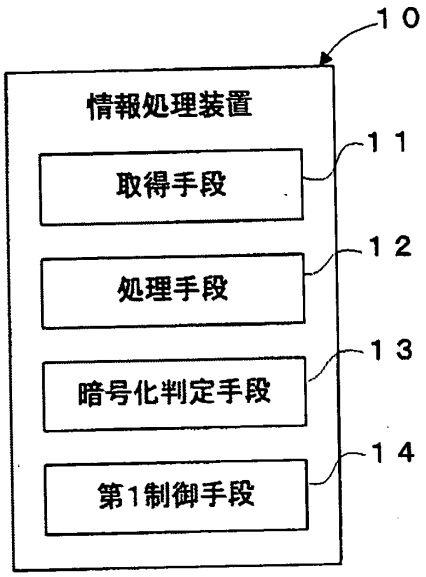
１０４…デコードモジュール

１１０…ＤＶＤ－ＲＯＭ

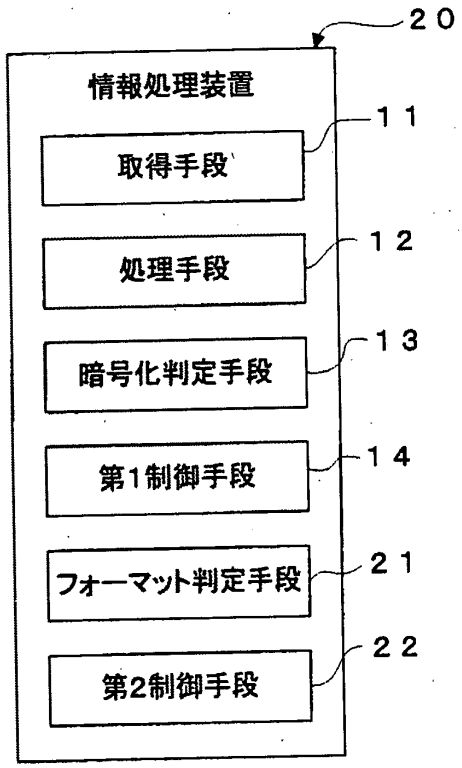
１１２…ゲームプログラム

【書類名】　図面

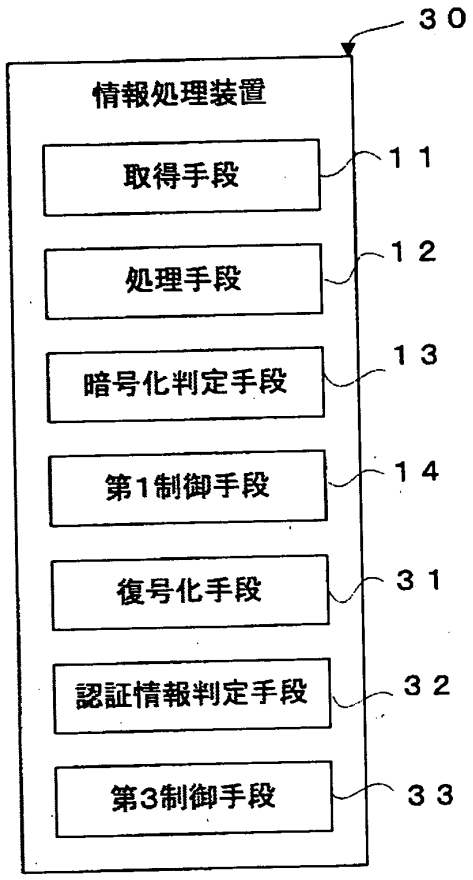
【図１】


１０
情報処理装置
１１
取得手段
１２
処理手段
１３
暗号化判定手段
１４
第1制御手段

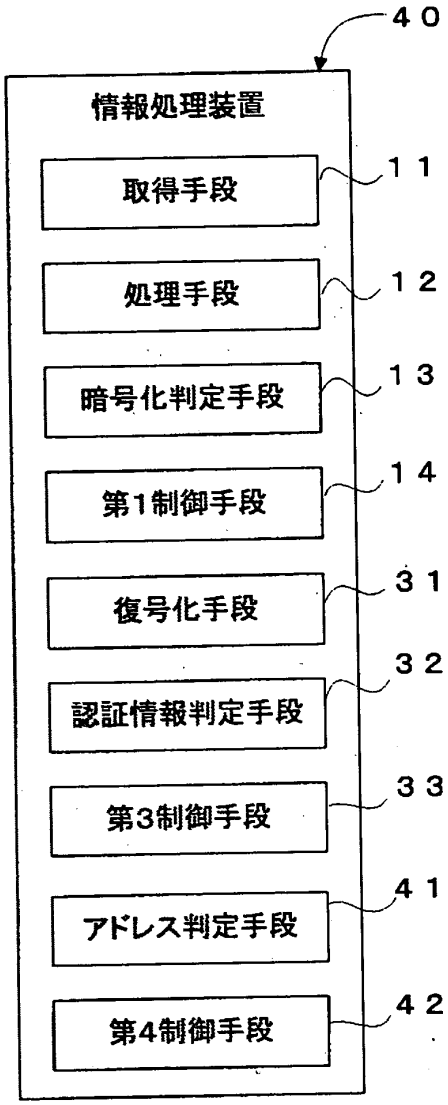
【図２】


２０
情報処理装置
１１
取得手段
１２
処理手段
１３
暗号化判定手段
１４
第1制御手段
２１
フォーマット判定手段
２２
第2制御手段

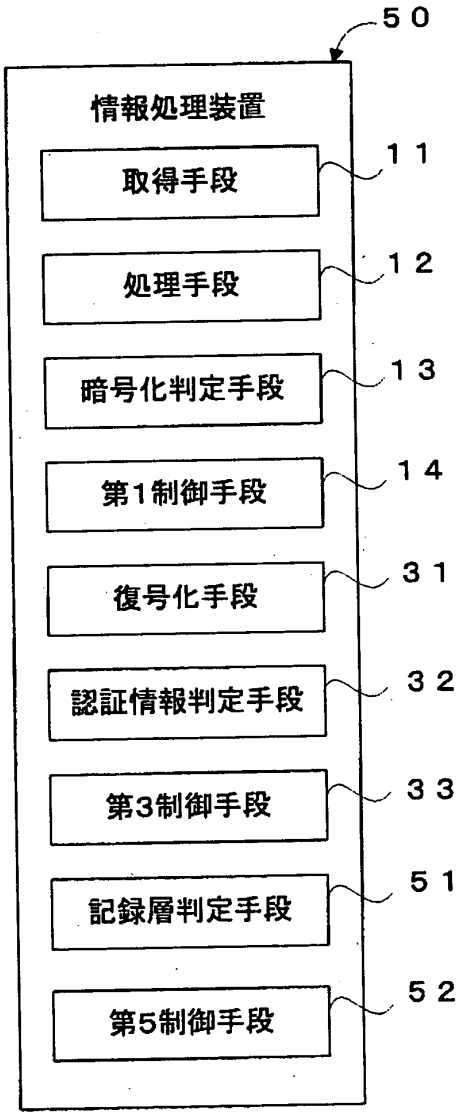
【図３】


３０
情報処理装置
取得手段
１１
処理手段
１２
暗号化判定手段
１３
第1制御手段
１４
復号化手段
３１
認証情報判定手段
３２
第3制御手段
３３

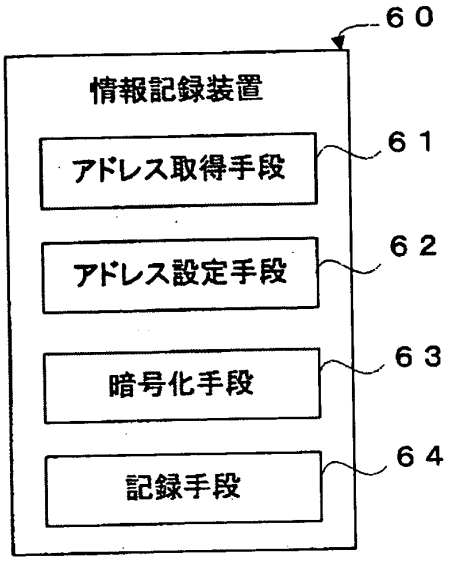
【図４】


４０
情報処理装置
取得手段
１１
処理手段
１２
暗号化判定手段
１３
第1制御手段
１４
復号化手段
３１
認証情報判定手段
３２
第3制御手段
３３
アドレス判定手段
４１
第4制御手段
４２

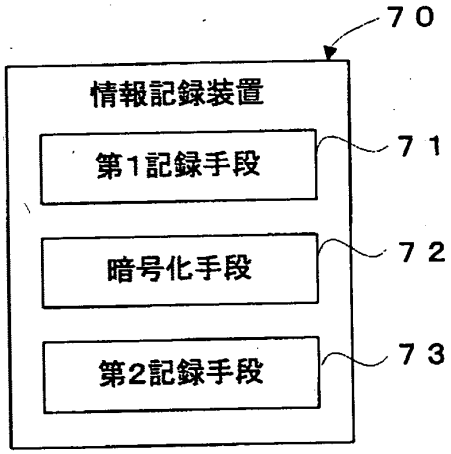
【図５】


５０
情報処理装置
取得手段
１１
処理手段
１２
暗号化判定手段
１３
第1制御手段
１４
復号化手段
３１
認証情報判定手段
３２
第3制御手段
３３
記録層判定手段
５１
第5制御手段
５２

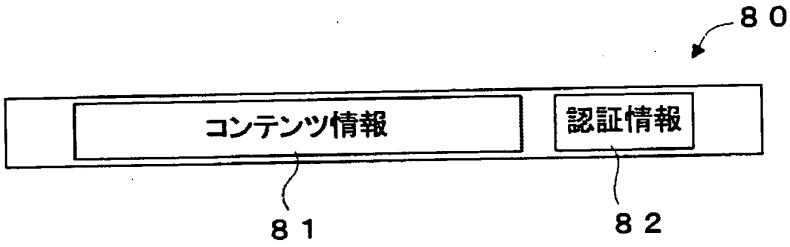
【図６】


６０
情報記録装置
アドレス取得手段
６１
アドレス設定手段
６２
暗号化手段
６３
記録手段
６４

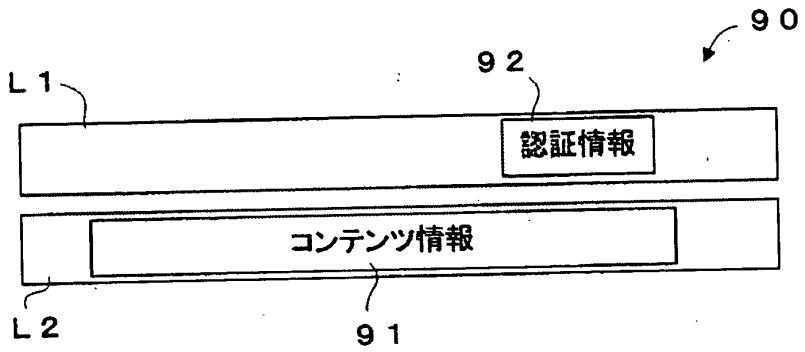
【図７】


７０
情報記録装置
第１記録手段
７１
暗号化手段
７２
第2記録手段
７３

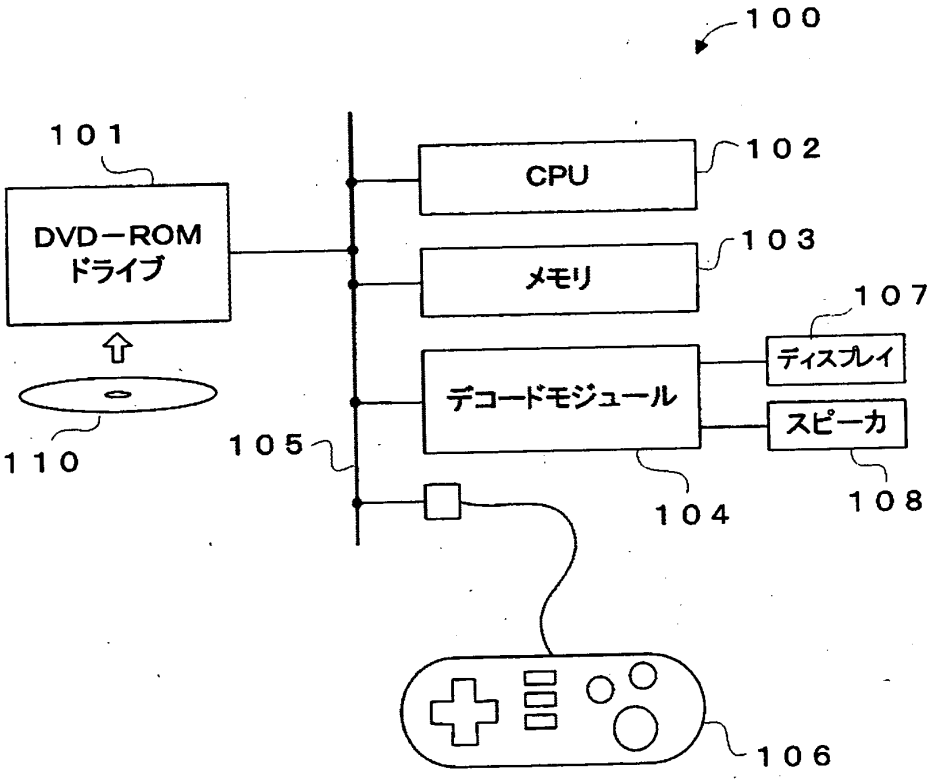
【図８】


８０
コンテンツ情報
認証情報
８１
８２

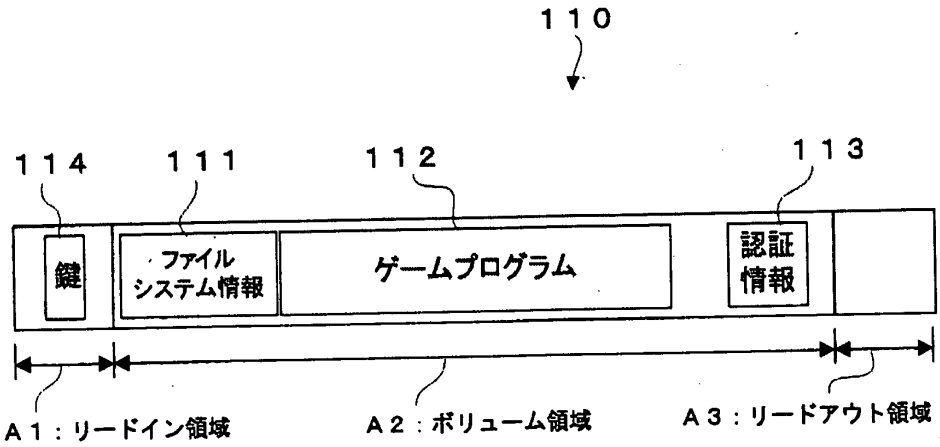
【図９】


９０
９２
Ｌ１
認証情報
コンテンツ情報
Ｌ２
９１

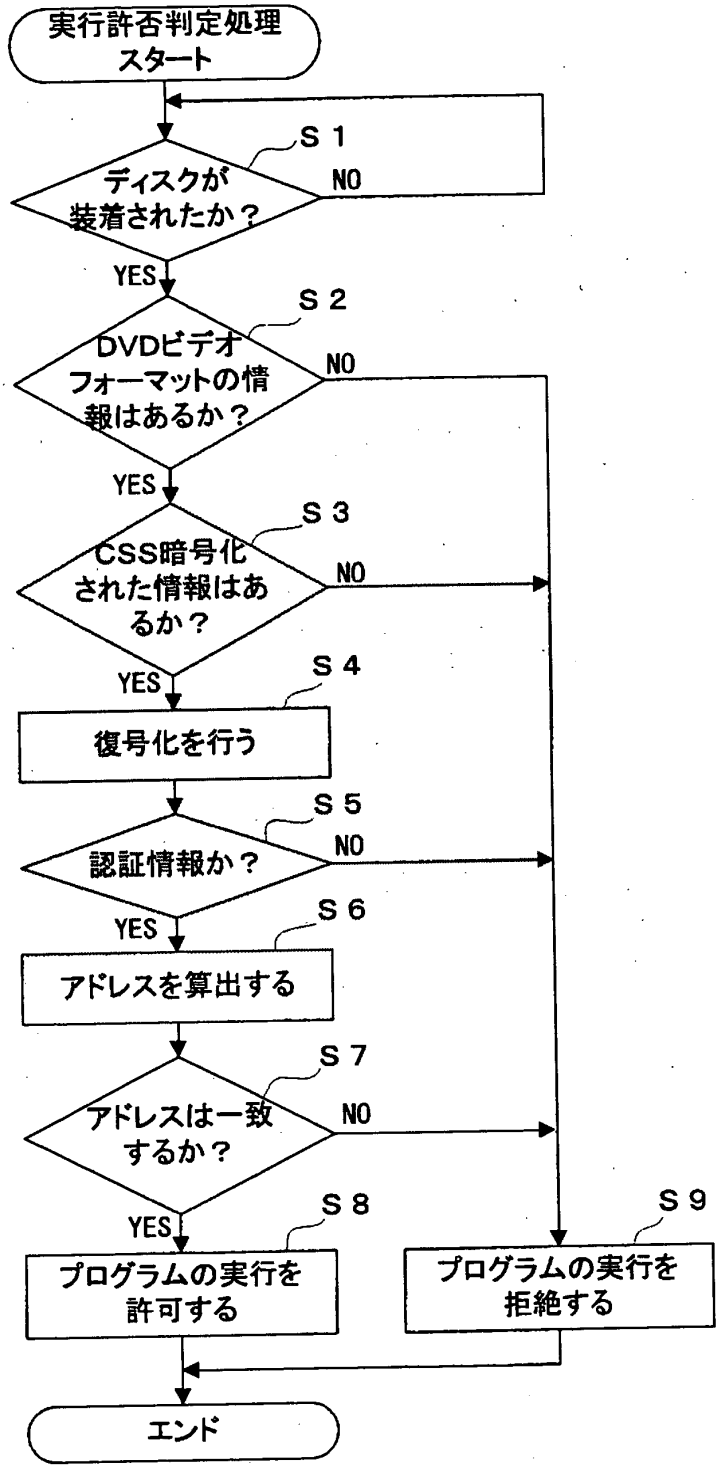
【図１０】


１００
１０１
DVD－ROM
ドライブ
１１０
CPU
１０２
メモリ
１０３
１０７
ディスプレイ
デコードモジュール
スピーカ
１０５
１０４
１０８
１０６

【図１１】


１１０
１１４
１１１
１１２
１１３
鍵
ファイル
システム情報
ゲームプログラム
認証
情報
Ａ１：リードイン領域
Ａ２：ボリューム領域
Ａ３：リードアウト領域

【図１２】


実行許否判定処理
スタート
S１
ディスクが
装着されたか？
NO
YES
S２
DVDビデオ
フォーマットの情
報はあるか？
NO
YES
S３
CSS暗号化
された情報はあ
るか？
NO
YES
S４
復号化を行う
S５
認証情報か？
NO
YES
S６
アドレスを算出する
S７
アドレスは一致
するか？
NO
YES
S８
プログラムの実行を
許可する
S９
プログラムの実行を
拒絶する
エンド

【書類名】　　要約書

【要約】

【課題】　不法コピー等に対する情報の保護を強化すると共に、これを低コストで実現する。

【解決手段】　コンテンツ情報に所定の暗号化方式で暗号化された認証情報を付加する。情報処理装置１０によってコンテンツ情報を実行又は再生するときには、取得した情報中に所定の暗号化方式で暗号化された情報が含まれるか否かを判定し、このような情報が含まれていないときには、コンテンツ情報を再生せず、実行せず又は出力しないようにする。

【選択図】　　図１

出証特２００３－３０５１４５０

出願人履歴情報

識別番号　〔０００００５０１６〕

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都目黒区目黒１丁目４番１号
氏　名　パイオニア株式会社